APPENDIX

MISSION-SPECIFIC CLOTHING AND EQUIPMENT

While in isolation, the SFOD carefully prepares clothing and equipment for its mission. They should be appropriate for the season, environment, and mission requirements. The clothing and equipment requirements vary widely from operation to operation whether the mission is under battlefield conditions or not. Discussion of each type of operation is beyond the scope of this manual. However, if SFODs conduct R&S, the information contained in this appendix provides overall considerations for mission-specific clothing and equipment.

CLOTHING

NOTE: After completing a mission, the detachment sergeant checks clothing and equipment using his premission clothing and equipment checklist, accounts for equipment, and notes where restocking and replacement are needed.

Prepare clothing to be used on the mission during isolation and have the SFOD operations sergeant check it. If the mission requires deniability, he should ensure that all uniform items are sterile, with all tags, labels, and identifying marks removed. Uniforms that are sun faded with fresh patch marks on them should not be used. Uniforms should be comfortable and serviceable. A flop brim bush cover with mosquito net helps break up the outline of the head and shoulders and offers protection. Wear jacket with the sleeves down and buttoned at the cuff and gloves. Doing so provides protection from thorns, bushes, and insects and camouflages the arms. Blouse trousers unless traveling through water. Most standard-issue U.S. combat boots leave a distinctive imprint, so consider wearing nonstandard footwear that leaves prints common to the operational area. Resoled boots can also serve this purpose.

WEARING AND CARRYING MISSION-ESSENTIAL EQUIPMENT

Use standard equipment so that if it becomes necessary to retrieve a particular item, time is not lost in searching for it. If possible, carry essential mission and survival gear in the pockets of the uniform. Arrange noncritical equipment carried to permit comfort and ease of access and handling. The actual items worn or carried vary widely with mission type and duration and climate.

Layering

While operating in a temperate or tropical battlefield environment, wear and carry equipment in layers: an outer layer, a middle layer, and an inner layer. This system can be adapted to other environments as dictated by METT-T.

Outer Layer. The outer layer is the rucksack, normally packed with the least essential items. If abandoned in a hurry, survival is still possible and the mission can

continue. In some cases, mission-essential equipment is too big and/or bulky to be carried elsewhere and must be carried in rucksacks (for example, radios, laser range finders, laser target designators, and like items). Items contained in or on the rucksack may normally include but are not limited to the following:

- Ponchos and/or rain jacket.
- Small camouflage net.
- Entrenching tool.
- Collapsible weed saw.
- Section of VS-17 panel, 1/3 meter by 2/3 meter.
- Poncho liner or sleeping bag.
- Ground pad (cold weather operations).
- Canteens.
- 550 cord and/or bungee cords.
- Rations.
- Insect repellent.
- Pursuit deterrent munitions (PDM) and claymore mines.
- Extra clothing.
- Extra ammunition and grenades (under the top flap of the rucksack).
- Smoke and CSN grenades (tied on the rucksack between the pockets).

NOTE: *For noise discipline, tape web gear at the buckles and other noisy spots.*

Middle Layer. The middle layer comprises the utility belt and/or LBE and weapon. Items contained in this layer include—

- Weapons. Weapons should be compatible with the AO and missions.
- Ammunition. Carry a basic combat load for each weapon. If the mission requires enemy contact, the load may be heavier.
- Grenades. Carry a mix of grenades for various purposes: fragmentation, CS, WP, thermite, and smoke.
- Pursuit deterrent munitions.
- Radio. Carry a radio for emergency contact (AN/PRC-1 ½). Each MSS, R&S site, or commo site should have at least one radio compatible with the rest of the SFOD's radios.
- Weapons cleaning kit. It should be compatible with weapons used by threat forces in the AO.
- Compass.
- Knife.
- Wire cutters.
- First aid pack. It contains two field dressings, one intravenous (IV) fluid set, and nonnarcotic pain killer (at a minimum).
- Poncho (if not carried in rucksack).
- Matches (in a waterproof container).
- Survival pouch. It should be mission-tailored and secured to the LBE to prevent loss if pockets become torn.
- Canteens. The number and capacity will depend on the weather and availability of water in the AO.

- Rations (for example, long-range reconnaissance patrol [LRRP] or MRE).
- Suspension line.
- Strobe light with infrared capability.
- Colored chemical lights.
- Flashlight with extra batteries.
- Night vision goggles with spare battery.
- Camera for the designated SFOD photographer.
- Small, tripod-mounted telescope or binoculars.
- Plastic flexicuffs (for securing prisoners).
- Extra socks.
- Cough suppressant (if operating in cold or wet environments).

Inner Layer. This layer comprises the hat and pockets of the uniform. It may also include—

- Lightweight battle-dress uniform (BDU) or the type of clothing customary to the AO.
- BDU cap or jungle hat.
- Map in waterproof container. The map should be unmarked so that if captured or compromised, it will not identify the detachment's AO.
- Wristwatch.
- Full-size and/or miniature compass.
- Notebook and mechanical pencil in a waterproof container. Ink notes and sketches can smear if they get wet, pencil carbon will not.
- Pen flare launcher with six flares of predetermined colors.
- A survival pouch, tailored to the area, containing such items as fish line and hooks, pocket knife, matches in a waterproof case, and/or a magnifying glass.
- Spare eyeglasses, if worn.
- Identification tags and medical tags (for emergency treatment, if an SFOD member is found unconscious). Tape these tags together so that they do not make noise.
- One pair of extra socks.
- Water purification tablets.
- Insect repellent in a leak-proof container.
- Cravat (may be worn around the neck).
- Gloves.

Items Not To Be Taken on a Mission. The following items should not be taken on an SR mission:

- Identification card (identification tags are sufficient, less compromising, and of less utility to threat forces).
- Official documents, including passes, memoranda, and the like.
- Personal letters, diaries, or notes.
- Tobacco products. Discarded cigarette butts, tobacco smoke, or stains on a trail can compromise the SFOD.

- Metal-capped cigarette lighters that make noise when opened or closed.
- Luminous tape. It is easily spotted for long distances at night with NVGs. In some situations, luminous tape can be used, but it should be attached with Velcro so it can be removed when not needed.
- Rings or ether jewelry with insignias.
- Weapons or equipment banned by the law of war.
- Any products not indigenous to the area or for which packaging is different from that found in the AO (for example, products packaged for U.S. sale).

APPENDIX

REPORT AND SURVEY FORMATS

The standard and nonstandard reports and formats found in this appendix are not designed to replace those found in the SOI issued during mission preparation. This appendix contains report and survey formats developed by both the U.S. Army and North American Treaty Organization (NATO). See Figures D-1 through D-12. This mixture of formats provides mission planners an expanded reference.

SPOTREP (REPORT OF ENEMY SIGHTING) FORMAT

Line	Content
SPOTREP	Include the subject line of message, DTG, and map series, sheet number, and edition, in that order.
ALPHA	Units of Measure.
BRAVO	Size. Give the number and type of threat forces using the following letter code:

Type Forces	Number Code
Infantry	A
Armored Personnel Carrier (APC)/Infantry Fighting Vehicle (IFV)	B
Tank	C
Field artillery	D
Antitank weapon	E
Antiaircraft weapon	F
Military truck	G
Light military vehicle	H

Figure D-1. Sample SPOTREP (report of enemy sighting) format.

Type Forces	Number Code
Helicopter	J
Aircraft	K
Radar	L
Command post	M
Minefield	N
Other tank obstacles	P
Other (followed by description)	Q

To pass the information, prefix the letter with the number of items. In the case of infantry, give the number of personnel seen; in the case of minefields, give the number of fields. Give the dimensions of minefields in DELTA. However, do not merely specify quantity. If reporting physical structures such as bunkers or trenches, specify the types of construction materials used and/or the structure's dimensions. If the amount cannot be determined, state "approximate number" before reporting the item in question.

CHARLIE Activity. Describe the activity of the threat force using the following numerical scale:

Type Activity	Number Code
On the move (followed by direction and speed)	1
Stationary but not dug in	2
In prepared positions	3
Other	4

State the items of equipment or machinery with which the threat is conducting the activity (for example, "Defensive positions being built with bulldozers").

DELTA Location. Identify the position of threat forces using grid reference or other agreed on system of reference. Use of the grid zone designator is important in eliminating confusion if the AO encompasses multiple grid zones. State if the target is in bunkers, caves, trenches, or thick brush.

ECHO Unit. Identify the threat force if it can be determined; if not, provide a description that might be helpful to the tasking agency. If a positive identification is made, indicate how identification was achieved. Describe the uniform (for example, note whether the uniform is brown spotted camouflage, black, or plain green, and with a helmet, soft cap, or beret [give the color]). Describe the patches on the uniform. If possible, describe any vehicle, aircraft, or watercraft markings, numbers,

Figure D-1. Sample SPOTREP (report of enemy sighting) format (continued).

or symbols (for example, an animal or other symbol that would indicate organization to intelligence analysts).

FOXTROT Time (DTG of sighting). Use local time and the standard 24-hour military clock. Do not convert to ZULU time.

GOLF Equipment. Identify or describe any weapons or equipment seen. If reporting on threat personnel with mixed types of small arms and/or other equipment, give the type and amount of each in BRAVO.

HOTEL Remarks. List any additional details that might help an intelligence assessment.

NOTE: The SPOTREP is a tactical intelligence report normally used in battlefield environments but useful in other environments as well. It is useful for reporting tactical information through the SOCCE when GP forces are closing with the SFOD and/or the SFOD and GP forces are integrated into the same operation.

Figure D-1. Sample SPOTREP (report of enemy sighting) format (continued).

TGTRECONREP (TARGET RECONNAISSANCE REPORT) FORMAT

1. **GENERAL.** One of the SFOD's most important products is the reconnaissance report on a specific target. Preparation of the report begins with the warning order and is completed as soon as the reconnaissance is complete. Format and composition of the report are described below. SFODs are often tasked with conducting a detailed reconnaissance in support of sabotage or other DA against a specific target. Usually, such targets are fixed industrial or military installations, but other types of targets can be surveyed as well.

2. **INFORMATION GATHERING AND PLANNING.** The first and probably most important part of a target reconnaissance report is information gathering and planning. Use the following sources to gather information:

   a. Latest edition maps:
      - 1:250,000 scale of the region where the target is located.
      - 1:50,000 scale covering a 20-NM radius around the target.
      - 1:25,000 scale of the target and surrounding area.

Figure D-2. Sample TGTRECONREP (target reconnaissance report) format.

- 1:12,500 scale of the target and specific points of interest.
- City maps, tactical commander's terrain analysis (TACCTA) maps, sketches, and special maps (if relevant and available).

b. Aerial and satellite photography.

c. Previous reports (for example, reconnaissance reports, agent reports, PW interrogation reports, open source literature, captured documents, area studies, and detailed installation analyses).

d. Personnel (for example, prisoners deliberately captured for information on the target and local inhabitants of the area).

e. OB, installation data, and overlays covering a 20-NM radius around the target. Minimum data required include—
- Ground OB.
- Air OB.
- Naval OB.
- Missile OB.
- Electronic OB.

f. When planning the reconnaissance, consider the following points:
- Time limitations.
- Time of the year.
- Weather (wetness in particular).
- Light data (including moon phase, first and last light).
- Route study to and from the target.
- Threat forces (in detail).
- Locals (hostile, friendly, and nonbelligerent).
- Friendly forces in the area.
- General and specific technical detail to be collected.
- Casualty handling procedures.

g. When planning the specific target surveillance, consider special equipment necessary for mission accomplishment. Examples include:
- Amphibious equipment.
- Binoculars.
- Camera (still, movie, video).
- Climbing and scaling aids.
- Night vision devices.
- Engineer's notebook.
- Writing utensil.
- Ruler and/or measuring tape.

Figure D-2. Sample TGTRECONREP (target reconnaissance report) format (continued).

3. **TARGET RECONNAISSANCE REPORT PREPARATION.** A target reconnaissance report is divided into seven parts. The first three parts contain sketches as part of the data and should be in sequence. All the information needs to be neatly and systematically recorded. Only by following this system will the information be detailed and accurate. Blanks are not filled in with guesswork, but are marked with a query (for example, "50 meters?" or "50 to 60 meters?").

PART ONE: Sketch Map (Situation Sketch). Include the following information in the sequence shown below:

a. Coverage of 500 square meters.

b. Name of reporter, unit, north magnetic arrow, grid reference, map sheet number, type of target, DTG, and scale used.

c. Other information:

- Wooded area (coniferous and/or deciduous).
- Rivers (direction, speed, and obstacles).
- Hills (severity of climbs).
- Habitation.
- Fences, hedges, ditches, gates.
- Ground conditions.
- Civilian and military vehicle movement (times, directions, and types).
- Threat forces locations.
- Target to be surveyed or attacked.
- Indication from which direction the target was observed before a detailed reconnaissance.
- Suggested patrol base and/or MSS.
- Any other pertinent information.

PART TWO: Side Elevation of Target. Include the following information:

a. Straight line diagram showing side elevation, plan, and end view of the target.

b. Scale used.

c. Side elevation diagram label to indicate the direction from which the target was viewed.

d. All relevant dimensions.

e. Estimates marked with a query.

f. Color of the target.

g. Access to the target.

Figure D-2. Sample TGTRECONREP (target reconnaissance report) format (continued).

h. Proposed charge placement and (if applicable) angle of cuts to be made.

i. Number of components.

j. Location of components (if not in plain view).

PART THREE: Cross-Sectional Diagram of Components to Be Attacked. Include the following information:

a. Diagram of all components.

b. Dimensions.

c. Components labelled by quantity.

d. Type of construction materials (wood, steel, plastic, or masonry).

PART FOUR: Explosives and Accessories. List any explosives, incendiaries, other devices, and accessories necessary for destruction or degradation of the target.

PART FIVE: Special Equipment. List any special equipment required (for example, boats, rope, ladders, and wire).

PART SIX: Security. Include the following information:

a. Strength of threat forces.

b. Alertness of threat forces.

c. Changing of guard times.

d. Communications (for example, telephone and radio).

e. Transport.

f. Weapons positions and command bunkers.

g. Fortifications, barrier scheme, and construction details.

h. Alarms and surveillance devices.

i. Dogs.

PART SEVEN: Unusual Occurrences. List all unusual and/or unexplained occurrences observed during the target reconnaissance. Include the presence of an unusually large guard force or the appearance of new structures at the target site.

Figure D-2. Sample TGTRECONREP (target reconnaissance report) format (continued).

ROUTEREP (ROUTES AND ROADS REPORT) FORMAT

Line — Content

ROUTEREP

Include the subject line of message followed by serial number and map series, sheet number, and edition, in that order.

ALPHA Units of Measure.

BRAVO Location. Give the location of the start and finish of that part of the route actually reconnoitered.

CHARLIE Type. Indicate the type of route by the following letter code:

Type Route	Letter Code
All-weather route	X
Limited all-weather route	Y
Fair-weather route	Z

Type X has the following characteristics:

- Is passable to all traffic in any weather except deep snow or flood.
- Has waterproof surfaces only.

Type Y has the following characteristics:

- Is limited to the volume of traffic in bad weather (for example, muddy shoulders).
- Does not have waterproof surfaces. These surfaces are considerably affected by rain, frost, thaw, or heat.

NOTE: Heavy unrestricted use during adverse weather may cause complete breakdown of these surfaces causing roads to be closed for short periods.

Type Z has the following characteristics:

- Is passable only in fair weather.
- Is impassable in bad weather.
- Cannot be kept open by maintenance short of major construction.

DELTA Military Classification. The SFOD engineers make this assessment using the following information as a guide:

Class 50 - Average traffic routes

Class 80 - Heavy traffic routes

Class 120 - Very heavy traffic routes

Figure D-3. Sample ROUTEREP (routes and roads report) format.

ECHO Width. Report the average width of a travelled way followed by the average width of grading. The "travelled way" is the hard surface of the road. The "width of grading" is the width of the travelled way plus the width of the hard shoulders. (For diagram see STANAG 2174.)

FOXTROT Route Constriction. List these routes individually and describe in the following order:

First: Nature of constriction.

Second: Location of constriction.

Third: Type of constriction shown as letter in the following letter code:

Type Constriction	Letter Code
Height of constriction	A
Width of constriction	B
Radius of curve of constriction	C
Gradient	D

Fourth: Dimensions of constriction using length/height unit of measure given in ALPHA.

Fifth: Bypass potential at constriction using the following letter code:

Type Bypass	Letter Code
Bypass easy. Local detour possible without engineer effort.	P
Bypass difficult. Bypass possible after engineer improvement.	Q
Bypass impossible.	R

NOTE: The critical heights, widths, radii of curvature, and gradients to be reported must be given in the SFOD's collection plan.

GOLF Concealment. Use the following numerical code to categorize the availability of concealment from the air:

Type Concealment	Number Code
Good concealment available at regular intervals along route.	1
Some concealment available.	2
Little or no concealment possible.	3

Figure D-3. Sample ROUTEREP (routes and roads report) format (continued).

HOTEL Special Considerations. Describe any other factors that may have to be considered by a force intending to use a route. The main meteorological obstacles are snow, flooding, and ice. Include other problems such as refugees and local traffic. Use the following numerical code to list hazards:

Type Hazard	Number Code
Snow (see below).	1
Flood (see below).	2
Ice. Ice conditions are present and may restrict movement.	3
Other. These hazards should be briefly described.	4

Use the following letter codes and suffixes to qualify snow and flood conditions:

Snow:

Qualification	Letter Code
No hindrance to wheeled vehicles.	P
Movement difficult for wheeled vehicles.	Q
Some digging or other route preparation may be necessary in places. Movement impossible for wheeled vehicles.	R

NOTE: The letter is followed by depth of snow in unit of measure given in ALPHA.

Flood:

Qualification	Letter Code
No hindrance to wheeled vehicles.	P
Movement difficult for wheeled vehicles.	Q
Some route preparation may be necessary in places. Waterproofing or fording gear is advisable. Movement impossible for wheeled vehicles.	R

NOTE: The letter is followed by depth of flood water over roads in unit of measure given in ALPHA.

Figure D-3. Sample ROUTEREP (routes and roads report) format (continued).

TACBEREP (TACTICAL BEACH REPORT) FORMAT

Line — Content

TACBEREP

Include the subject line of message and serial number followed by code name, map series, sheet number, and edition, in that order.

ALPHA Units of Measure.

BRAVO Offshore Obstructions. Include previously unknown offshore obstructions showing above water at low water. Give a description of their positions using grid references or bearings and ranges from known landmarks or charted reference points.

CHARLIE Littoral Drift. When the littoral drift significantly differs in velocity or direction from earlier estimations, indicate the new velocity in knots to the nearest 1/10 knot (one knot equals approximately 31 meters per minute). Littoral drift is current moving generally parallel and adjacent to the shoreline. Express the direction of the current flow as the LEFT or RIGHT. Direction always refers to the beach area viewed from seaward.

DELTA Datum Point(s) (DP). Indicate the DPs as required by the existing situation. These points are fixed position(s) to which sounding lines are related. The existing situation will dictate whether one or more DPs will be required. DPs are designated by letters, (for example, DP A, DP B, DP C). Each DP must be "fixed" and reported by grid references (8 digits if possible), or by bearings and ranges, or by cross bearings from known landmarks or charted reference points.

ECHO Sounding Interval. Give the distance between each sounding on a sounding line. The sounding interval may be varied by particular units, specific conditions, or the requirements of the command employing the SFOD.

FOXTROT Sounding Lines. Use the following information to indicate sounding lines:

1. Each sounding line is numbered: F1, F2, and F3. The information relating to these sounding lines is provided in five subparagraphs (a through e), each reporting separate types of information. The sounding line designation consists of three characters. The first character is the letter designating the DP to which the sounding line is related. The second and third characters are two digit numbers that designate the sequential number of individual sounding lines (for

Figure D-4. Sample TACBEREP (tactical beach report) format.

example, A01, A02, A03, B01, and B02). The subparagraphs a through e provide the following information:

a. Locates the water line at the time of sounding (WLTS) in relation to the applicable DP and is expressed as bearing range from the DP. (The DP will always be on the bearing of the first sounding line).

b. Indicates the bearing of the sounding line as viewed from seaward.

c. Indicates the DTG (the month and year are not required).

d. Indicates the distance (in the unit of measure selected in ALPHA) and WLTS to the back of beach (BOB) and the vertical rise over this distance along the bearing of the sounding line. BOB is that part of the shoreline, normally well defined, where extreme stormwave action ends and hinterland vegetation begins. Where there are cliffs or walls and other man-made barriers, they will normally be designated the BOB. If the vertical rise cannot be established, then the gradient should be estimated using the following letter code:

	Gradient	Letter Code
Flat	Flatter than 1:20	V
Mild	1:61 to 1:20	W
Gentle	1:31 to 1:60	X
Moderate	1:15 to 1:30	Y
Steep	Steeper than 1:15	Z

e. Indicates each sounding to the nearest 1/5 meter. The soundings must be reported in linear sequence commencing from WLTS and working seaward.

2. For the second and subsequent sounding lines, the report will show similar data except that, under subparagraph a, the WLTS may be expressed by—

a. Indicating the bearings and distance from the WLTS of previous sounding line.

b. Indicating the bearing and distance from the DP.

c. Using the same procedure as in FOXTROT 1.a if any sounding line is to be based on a new DP.

GOLF Underwater Obstacles. Indicate the underwater obstruction relative to sounding lines by naming the type of obstruction.

HOTEL General Beach Composition. Describe the beach as a whole. The beach is divided into two parts: the foreshore (mean low water [MLW] to mean

Figure D-4. Sample TACBEREP (tactical beach report) format (continued).

high water [MHW]) and the backshore (MHW to BOB). Include an assessment of underwater composition. Use the following letter code:

Beach Composition	Letter Code
Mud	A
Clay	B
Sand - up to pinhead size	C
Gravel (shingle) - up to top of thumb size	D
Pebbles - up to clenched fist size	E
Cobbles - up to human head size	F
Boulders - larger than human head	G
Rock	H
Coral	J

NOTE: If there is marked variation in composition along the beach, this fact is to be reported using code by reference to designated sounding line numbers (for example, H.I.A08 to B02E, that is, foreshore line A08 to B02 now composed of pebbles).

JULIET General Trafficability of Beach. Indicate the general trafficability of the beach. Consider only the following two areas of the beach: the portion between WLTS and MHW and the backshore. The color of soil and vegetation often gives an indication of the trafficability in an area. Some examples follow:

a. Light colored soils usually indicate good drainage. Examples are chalk (unless badly broken up), gravel, and sand. These soils usually provide good going for vehicles.

b. Brown soils generally provide good going unless wet. Dark brown soils, in particular, tend to be sticky and heavy when wet and often have a treacherous surface crust.

c. Red soils are uncertain. Those derived from sandstone or limestone usually provide good going, although dull red or purple clay soils are almost impassable when wet.

d. Grey slate-colored soils are typical of clay. They provide generally good going except if wet, when they may be impassable to heavy vehicles.

e. Black soil usually denotes bad going. It can indicate peat or boggy ground; such ground should be avoided until a safe route has been reconnoitered.

f. Bright green patches or grass or vegetation in an otherwise uniform tract usually gives warning of soft areas that are to be avoided.

Figure D-4. Sample TACBEREP (tactical beach report) format (continued).

Use the following letter code:

Trafficability Code	Letter Code
Firm - can be used by 2-wheel drive vehicles or 4-wheel drive vehicles and trailers, unless heavy and continuous use is intended.	W
Moderate - can be used by military 3-or 4-ton vehicles which should be able to start from rest using 4 wheel drive. Beach matting and/or roadway is recommended.	X
Soft - cannot be used by 4-wheel drive vehicles to start from rest but might be able to cross a soft patch if already moving. Beach matting and/or roadway is recommended.	Y
Very Soft - cannot be passed with wheeled vehicles. Tracked vehicles may experience difficulty. Beach matting and/or roadway is required (for example, J.1.X2Z).	Z

NOTE: If there are marked differences in trafficability along the beach, they are to be reported in a similar manner to HOTEL, above (for example, J.1.A08 and B02 Y, that is, foreshore trafficability now assessed at SOFT between lines A08 and B02). Trafficability can only be assessed as above WLTS. It must be clearly understood that a correct assessment of trafficability cannot be guaranteed, bearing in mind conditions under which the reconnaissance party may be working.

KILO Exits. Describe any new exit(s) or exit(s) that have changed. Describe the beach exit point only where it meets BOB. Use the following letter code to describe exits:

Exit Code	Letter Code
Infantry - if the exit is usable by infantry only, the width is given.	A
Tracked - if the exit is usable by both infantry and tracked vehicles then the width is given followed by the appropriate trafficability code in JULIET above.	B
Wheeled - if the exit is usable by infantry and other vehicles then the width is given followed by the appropriate trafficability code.	C

Figure D-4. Sample TACBEREP (tactical beach report) format (continued).

Exit Code	Letter Code
Unusable - if the exit is unusable then a new exit that would take both wheeled and tracked vehicles 10 meters wide and assessed as SOFT would be signalled as follows: K.1.2782418C 10Y	D

LIMA Position of Beach Reconnaissance Team. Give the position of an SFOD after completing its reconnaissance as a 6-digit grid reference or by some other previously arranged system of reference.

MIKE Enemy. Indicate if the enemy has been seen or contacted stating YES in the unit report and submit a detailed SPOTREP separately. State NIL if no enemy has been seen or contacted.

NOVEMBER Remarks. List any additional relevant information.

NOTE: If there is a preexisting beach survey report and no change is found in the information, the relevant paragraph or subparagraph heading followed by no change (NC) is sent (for example, J.1.XZNC).

Figure D-4. Sample TACBEREP (tactical beach report) format (continued).

SURFREP (SURF REPORT) FORMAT

Line	Content

SURFREP
Include the subject line of message and serial number followed by code name and map series, sheet numbers, and edition, in that order.

ALPHA Units of Measure.

BRAVO Time. State DTG of completion of surf observation.

CHARLIE Significant Breaker Height. State the average height observed in unit of measure shown in ALPHA of the highest one third of all breakers observed in a 10-minute period (expressed to the nearest 1/5 meter).

DELTA Maximum Breaker Height. State the largest breaker observed expressed in unit of measure shown in ALPHA.

ECHO Period. State the time between breakers to nearest second.

Figure D-5. Sample SURFREP (surf report) format.

FOXTROT Breaker Types. Show the number of each type of wave followed by the letter code of that type of wave as indicated below:

Breaker Type	Letter Code
Spilling: The wave becomes unstable and forms white water at the crest. The white water (foam) expands slowly down the front face of the breaker. Breaking action is mild.	A
Plunging: The wave crest advances so much faster than the base of the wave that it falls almost into the trough with a violent action. The resulting foam appears almost instantly over the complete front. At times, air is caught in the breaker as it tumbles forward, creating a type of explosion.	B
Surging: The wave crest tends to advance faster than the base of the wave, suggesting the formation of a plunging breaker. However, just before breaking completely, the base advances faster than the crest and the plunging is arrested. These crests are generally found at steep gradients.	C

GOLF Angle and/or Direction. State the acute angle that forms between the breaker lines and the shoreline (expressed to the nearest 5 degrees). Express the breaker direction as the direction towards which the breaker is moving as R (right) or L (left) of the observer when he is facing from seaward.

HOTEL Littoral Drift (Inshore Current). Express the speed of the current moving generally parallel and adjacent to the shoreline in the velocity unit of measure specified in ALPHA. This number is followed by the letter R (right) or the letter L (left) to indicate the set (direction) of this current. This set is expressed as the direction towards which the current is flowing (as observed from seaward).

JULIET Lines of Breakers and Width of Surf Zone. Express the number of well defined breaker lines in the surf zone using length unit of measure specified in ALPHA. The width is the distance from the outermost breaker to the extreme uprush of water on the beach.

KILO Remarks. Include special factors that could affect the above report (for example, strong winds and restricted visibility).

Figure D-5. Sample SURFREP (surf report) format (continued).

DELTREP (RIVER/ESTUARY REPORT) FORMAT

Line — Content

DELTREP

Include the subject line of message and serial number followed by map series, sheet numbers, and edition, in that order.

ALPHA Units of Measure.

BRAVO Location (area covered by report). Use grid references.

CHARLIE Main Channel. Show in the following numbered sequence:

1. Location. Give the grid reference of the entrance to the main channel.
2. Seaward Approach. State the bearing from seaward of approaches to the main channel.
3. Reference Points. "Fix" the entrance to the main channel by means of transits and/or bearing of prominent features from seaward. These features must be recognizable on a map or chart. Report as follows:
   a. Prominent Features. Describe and give the position of the feature followed by its bearing from seaward. If more than one, number them 1, 2, and 3.
   b. Transits. Describe and give the position of first point followed by a description and position of second point. If more than one set, number them 1, 2, and 3.

DELTA Buoys. Show local system of buoys (if any) or markings placed by the SFOD as follows:

Buoy Number	Code
Starboard buoys - shape and color (if any).	1
Port buoys - shape and color (if any).	2
SFOD placed markers - description and location.	3

ECHO Hazards. Tabulate in the following numerical code:

Hazard	Number Code
Sandbars	1
Wrecks	2
Rocks	3
Tidal races	4
Other obstacles	5

NOTE: Locate the hazards with a 6- or 8-digit grid reference and briefly describe them.

Figure D-6. Sample DELTREP (river/estuary report) format.

FOXTROT Navigable Limits. Give the limits that are the highest points upstream in the main channel with the following depths at low water:

Depth	Number Code
2 meters	1
1 meter	2
1/2 meter	3

GOLF Beaching and Landing Points and Their Exits. Describe these points in the following order:

First: Grid reference.

Second: Indicate the type of craft that can use the landing point by the following number code:

Type Vessel	Number Code
Landing Craft Medium/Utility	1
Landing Craft Personnel	2
Shallow draft boats with outboard motors	3

Third: Indicate the overall trafficability of the beaching point and exit by using the following letter code:

Trafficability	Letter Code
Firm - can be used by 2-wheel drive vehicles or 4-wheel drive vehicles and trailers, unless heavy and continuous use is intended.	W
Moderate - can be used by military 3-or 4-ton vehicles that should be able to start from rest using 4-wheel drive. Beach matting and/or roadway is recommended.	X
Soft - cannot be used by 4-wheel drive vehicles to start from rest, but might be able to cross a soft patch if already on the move. Beach matting and/or roadway is recommended.	Y
Very Soft - cannot be used by wheeled vehicles. Tracked vehicles may experience difficulty. Beach matting and/or roadway is required.	Z

NOTE: If the beaching or landing point or its exit is unsuitable for any vehicles, no trafficability code letter is passed.

HOTEL Current. Indicate the speed of the current and/or tidal stream in the unit of measure shown in ALPHA as follows: velocity,

Figure D-6. Sample DELTREP (river/estuary report) format (continued).

direction in which flowing (by use of letters indicating one of the eight points of the compass, for example, SE or W), DTG, and location (grid reference). If necessary to show variation, give several of these units of measure.

JULIET Texture of River Bed. Give this information in the following order:

First: Grid reference.

Second: Letter code indicating composition of river bed as follows:

Texture	Letter Code
Mud	A
Clay	B
Sand (up to pinhead size)	C
Gravel (up to top of thumb size)	D
Other (followed by description)	E

KILO Remarks. Give any other important information in this paragraph.

Figure D-6. Sample DELTREP (river/estuary report) format (continued).

BRIDGEREP (BRIDGE REPORT) FORMAT

Line — Content

BRIDGEREP

Include the subject line of message followed by serial number and map series, sheet numbers, and edition.

ALPHA Units of Measure.

BRAVO Location. Give the grid reference of the bridge followed by engineer classification, if known.

CHARLIE Horizontal Clearance. State the minimum clear distance between the inside edges of the bridge structure beginning at 30 centimeters above the road and continuing upwards.

DELTA Under Bridge Clearance. Give the height of clearance in unit of measure in ALPHA. State the maximum clear distance between the underside of the bridge and the surface of the ground or of the water. If the water is tidal, include the DTG of measurements.

Figure D-7. Sample BRIDGEREP (bridge report) format.

ECHO Spans.

First: Show the number, material, and type of span construction for each span by number and letter symbols.

Second: List spans in sequence starting from the west. If the bridge is running close to north-south, list the spans from the north and insert the letter N before the numbers and letters.

Third: Show material of span construction in the following letter code:

Material	Letter Code
Steel or other metal	A
Concrete	K
Reinforced concrete	AK
Prestressed concrete	KK
Stone or brick	P
Wood	H
Other types	O

Fourth: Show the type of span construction for each span in the following numerical code:

Span Type	Number Code
Truss	1
Girders	2
Beams	3
Slab	4
Arch (closed spandrel)	5
Arch (open spandrel)	6
Suspension	7
Floating	8
Swing	9
Bascule	10
Vertical lift	11
Others	12

FOXTROT Length and Condition of Spans. List and number length of individual spans in order reported in ECHO above. If any spans are damaged, classify them in the following letter code:

Type Damage	Letter Code
May be significantly damaged but probably capable of supporting light vehicles.	A

Figure D-7. Sample BRIDGEREP (bridge report) format (continued).

Type Damage	Letter Code
Impassable to traffic but span not totally destroyed.	B
Span destroyed.	C

GOLF Overall Length. Give the length in units of measure shown in ALPHA (it may be different from the sum of the span lengths).

HOTEL Roadway Width. Give the width in units of measure shown in ALPHA.

JULIET Overhead Clearance. Give the clearance in units of measure shown in ALPHA at the following points in this order:

- Left shoulder.
- Center of roadway.
- Right shoulder.

NOTE: If all clearances are equal, report figure once only. If there is unlimited clearance, omit this paragraph.

KILO Bridge Bypass. Give the information in the following sequence:

First: State overall potential in the following letter code:

Type Bypass	Letter Code
Bypass easy. The obstacle can be crossed within the immediate vicinity of the bridge without work to improve the bypass.	P
Obstacle can be crossed within the immediate vicinity of the bridge but some work will be necessary to prepare the bypass.	Q
Bypass impossible. Crossing of the obstacle is only possible by a detour some distance from the original site.	R

Second: Show location by grid reference.

Third: Give a brief description of the nature of bypass.

Fourth: List any restrictions including dimensions in units of measure shown in ALPHA.

LIMA Remarks.

Figure D-7. Sample BRIDGEREP (bridge report) format (continued).

TECHNICAL INTELLIGENCE EXPLOITATION PLAN AND CATEGORY REQUIREMENTS FORMAT

This report includes an exhaustive listing of exploitation categories and collection requirements regarding items of interest to battlefield TECHINT units. This report shows how TECHINT requirements are generated. SFODs engaged in SR need to be prepared to submit TECHINT reports on modified or new items encountered.

PRELIMINARY REQUIREMENTS FOR EXPLOITATION

The preliminary requirements for exploitation are:

- Determining safety requirements.
- Examining additional information requirements.
- Determining intended recipient of intelligence.
- Formulating detailed project timeline for assessment format.
- Conducting a leader's reconnaissance of subject to be assessed and the area of the assessment.

GENERAL EXPLOITATION PLAN

The general exploitation plan covers—

- Initial photography. Preliminary photographs of outside and inside (show status of equipment before assessment).
- Inventory.
  - Examine system for any written information (documents, operator manuals, maps), data plates, or operating instructions.
  - Identify all individual components requiring separate analysis.
- If equipment requires further analysis, determine exploitation category and proceed.

EXPLOITATION CATEGORY REQUIREMENTS

Mobility Requirements

Track Vehicles

List of subcategories.

- Infantry fighting vehicles.
- Cargo or transport.
- Armored personnel carrier.
- Tank chassis.
- Self-propelled howitzer.
- Self-propelled rocket launcher.
- Tank destroyer.
- Self-propelled antiaircraft.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format.

Main category requirements.

- Type of vehicle.
- Engine type.
- Cooling system.
- Power train description.
- Brake system.
- Suspension system.
- Steering system.
- Vehicle description.
- Electrical system.
- Physical dimensions.

Subcategory requirements.

- Infantry fighting vehicle:
  - Type of armor.
  - Armor thickness.
  - Maximum personnel seating capability.
  - Location and number of firing ports.
  - Location of hatches.
- Cargo or transport:
  - Cargo compartment size.
  - Maximum height carrying capability.
  - Maximum personnel seating capability.
  - Type of cargo vehicle is designed for.
- Armored personnel carrier:
  - Type of armor.
  - Armor thickness.
  - Maximum personnel carrying capability.
  - Location and number of firing ports.
  - Location of hatches.
- Tank, howitzer, self-propelled rocket launcher, or tank destroyer:
  - Type of armor.
  - Armor thickness.
  - Body design.
  - Number of road wheels and support rollers.
  - Turret location.
  - Type of track.
  - Location of hatches.
  - Power pack location.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Wheeled Vehicles

List of subcategories.

- Reconnaissance vehicles.
- Cargo or transport vehicles.
- Armored personnel carrier.
- Infantry fighting vehicles.

Main category requirements.

- Type of vehicle.
- Vehicle description.
- Physical dimensions.
- Engine type.
- Cooling system.
- Power train description.
- Electrical system.
- Brake system.
- Suspension system.
- Steering system.

Subcategory requirements.

- Reconnaissance vehicles:
  - Maximum personnel seating.
  - Armor thickness.
  - Special exhaust system.
- Cargo or transport vehicles:
  - Cargo compartment size.
  - Maximum weight-carrying capability.
  - Maximum personnel seating compartment.
  - Type of cargo vehicle is designed for.
- Armored personnel carrier:
  - Armor thickness.
  - Maximum personnel seating capability.
  - Location and number of firing ports.
  - Location of hatches.
  - Type of armor.
- Infantry fighting vehicle: Same as above.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Engineer Equipment

List of categories.

- Clearing equipment.
- Ditching equipment.
- Water and/or gap crossing equipment.
- Air compressor.
- Power supply equipment.
- Special purpose equipment.

Main category requirements.

- Type prime mover.
- Vehicle description.
- Physical dimensions.
- Engine type.
- Cooling system.
- Power train description.
- Brake system.
- Suspension system.
- Electrical system.
- Steering system.

Subcategory requirements.

- Clearing equipment:
  - Type.
  - Crew.
  - Power.
  - Capabilities.
- Ditching equipment: Same as above.
- Water and/or gap crossing equipment:
  - Crew.
  - Capacity.
  - Power.
  - Type.
  - Width of bridge.
  - Height of bridge.
  - Length of bridge.
  - Spanning length.
- Power supply equipment.
  - Type.
  - Power.
  - Capabilities.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Subcategory requirements (continued):

- Air compressor: Same as above.
- Special purpose equipment: Same as above.

Rotary Wing Aircraft

List of subcategories.

- Cargo and/or transport.
- Attack and/or assault.

Main category requirements.

- Body type.
- Main rotor system.
- Tail rotor system.
- Landing gear.
- Fuel system.
- Engines.
- Cooling system.
- Electrical system.
- Cargo compartment size.
- Cargo loading and/or unloading system.
- Maximum personnel seating.
- Maximum weight-carrying capability.
- Flight controls.
- Armor.
- Internal weapons mounts.

Subcategory requirements.

- Cargo and/or transport: External winch platform.
- Attack and/or assault:
  - Weapons mounts.
  - Machine guns.
  - Rockets.
  - Bombs.
  - Antitank guided missiles.
  - Target acquisition.

C-E REQUIREMENTS

Communications

List of subcategories.

- Radio.
- Line equipment.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Vehicular mounted or manpack.
- Location found (building, van, field, or house).
- Data plate information (nomenclature, serial number, year of manufacture).
- Power requirement.
- Planning range and/or range of operation.

Subcategory requirements.

- Radios:
  - Radio frequency power output.
  - Types of antennas used.
  - Modes of operation.
  - Frequency range.
  - Tuning method (continuous or detent).
  - Preset frequencies (yes or no, how many).
  - Batteries.
  - External antenna matching unit.
  - Number of power supplies.
  - Remote capability.
  - Retransmission capability.
  - Type of radio (transceiver, receiver, or transmitter).
  - Types of modulation (AM or FM).
  - Morse code capability.
  - Frequency hopping capability.
- Line equipment:
  - Wire thickness.
  - Ringer capability.
  - Line handling capability.
  - Motor speed.
  - Words per minute transmission.
  - Line current.
  - Size of paper used.
  - Reperforator capability.
  - Built-in operator pack.
  - Length and diameter of patch cord.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Radar

List of subcategories.

- Air traffic control.
- Weather.
- Ground surveillance.
- Fire control.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found (airport, battlefield, house, van).
- Data plate information.

Electronic Warfare

List of subcategories.

- Jammers.
- Direction finders.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found.
- Vehicular mounted or manpack.
- Data plate information.
- Power requirements.
- Frequency range.
- Frequency hopping capability.

Subcategory requirements.

- Jammers:
  - How many bandwidths can they jam at one time?
  - What is strength of jamming signal?
  - Can it jam radars and communications?
- Direction finders:
  - Can it locate a target alone?
  - How long does it take to locate a target?
  - Is it an automatic or manual direction finding unit?

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Electronic Devices

List of subcategories.

- Searchlights.
- Starlight scopes.
- Mine detectors.
- Distance measuring devices.
- Wind and/or weather measuring devices.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found.
- Data plate information.
- Power requirement.
- Vehicular mounted or manpack.

Subcategory requirements.

- Searchlights:
  - What is the candlepower rating?
  - What is the range of the light?
- Starlight scopes:
  - What is the range it can detect someone or something?
  - What is the minimum amount of light required to operate?
  - Is it a transmitter and a receiver?
  - Can it be mounted on a weapon as well as handheld?
- Mine detectors:
  - What is the depth it can detect items in soil?
  - What is the depth it can detect items in water?
  - Can it detect metallic and/or nonmetallic mines?
  - How many transmitters does it have?
  - How many receivers does it have?
- Distance measuring devices:
  - What is the maximum distance it can measure?
  - What is the minimum distance it can measure?
  - Can it measure in metric and American standards?

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

- Wind and/or weather measuring devices:
  - What is the maximum wind speed it can measure?
  - What is the minimum wind speed it can measure?
  - What type of weather measurements will it give?
  - Does it give a printout of the weather report?

CHEMICAL, MEDICAL, AND LOGISTIC (CML) REQUIREMENTS

Detectors

List of subcategories.

- Chemical and/or biological detection and identification kits and sets.
- Radiation detection and measuring instruments.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Vehicular or manpacked.
- Location found (building, van, field, house).
- Data plate information (nomenclature, serial number).
- Planning range and/or range of operation.
- Power requirements.
- Inventory.
- Photographs.

Subcategory requirements.

- Chemical and/or biological detector and identification kits and sets:
  - What agents will they detect or identify?
  - Do they have remote capabilities?
  - How easy are they to use?
  - How effective are they?
  - What levels of agents can they detect?
  - Can detectors distinguish agents?
  - Can kits identify multiple agents at the same time?
  - Will they sample air, soil, water (which one or ones)?
- Chemical or biological detectors and alarms:
  - What agents will they detect?
  - Do they have remote capabilities?
  - How easy are they to use?
  - How effective are they?

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

- Chemical or biological detectors and alarms (continued):
  - Type of alarm (audio or visual).
  - Time of contact between sampling and alarm.
- Radiological dosimeters and dosimeter sets:
  - What equipment is required?
  - What is the total dose measured?
  - Do they measure present or total doses?
  - What type of radiation is measured?
- Radiological area survey meters:
  - What type of radiation is measured?
  - Are they manpack, aircraft, or vehicle mounted?
  - How is equipment operated?
  - What type of radiation is detectable?
- Radiological low-level radiation detection meters:
  - What type of radiation is detectable?
  - What level is measureable?
  - How does equipment measure radiation?

Decontamination Equipment

List of subcategories.

- Individual decontamination kits.
- Portable decontamination apparatuses.
- Vehicle mounted decontamination apparatuses.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found (building, van, field, house).
- Data plate information.
- Power requirement.
- Inventory.
- Photographs.

Subcategory requirements.

- Individual decontamination kits:
  - How many times can they be used?
  - What type of decontaminants do they use?
  - What agents are they used against?

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

- Individual decontamination kits (continued):
  - How easy are they to use?
  - How effective are they?
- Portable decontamination apparatuses:
  - How is equipment transported?
  - What type of decontaminants are used?
  - What agents are they used against?
  - How easy are they to use?
  - How effective are they?
  - What amount of equipment can they decontaminate?
  - Is extra equipment needed to support operation?
- Vehicle mounted decontamination apparatuses:
  - Where are they mounted?
  - What type of decontaminants are used?
  - What agents are they used against?
  - How many crew members are required?
  - How effective are they?
  - What amount of equipment can they decontaminate?
  - Is extra equipment needed to support operation?

Protection Equipment

List of subcategories.

- Individual protection.
- Collective protection.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found.
- Data plate information.
- Power requirement.
- Inventory.
- Photographs.

Subcategory requirements.

- Individual protection:
  - What protection is afforded?
  - How is equipment used?

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

- Individual protection (continued):
  - How effective is equipment?
  - What type of filter is used, if any?
  - How easy is it to maintain?
- Collective protection:
  - What protection is afforded?
  - How is equipment used?
  - How effective is equipment?
  - What type of filtering system is used?
  - How easy is it to maintain?
  - How many personnel can system accommodate?

Smoke Systems

List of subcategories.

- Hand grenade.
- Smoke pot.
- Smoke drum.
- VESS.
- Smoke generator.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found.
- Data plate information.
- Power requirement.
- Inventory.
- Photographs.

Subcategory requirements.

- Hand grenade:
  - Is it signaling smoke?
  - What is the duration of smoke?
  - How effective is the smoke?
  - Does the smoke contain any additives?
- Smoke pot:
  - What is the burn time?
  - How effective is the smoke?

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

- Smoke pot (continued):
  - Can the pots be stacked?
  - Is it a floating smoke pot?
  - Does the smoke contain any additives?
- Smoke drum:
  - What is the burn time?
  - How effective is the smoke?
  - Is it a floating drum?
  - Does the smoke contain any additives?
- VESS:
  - How effective is the smoke?
  - How much of the vehicle fuel supply is required?
  - Does the smoke contain any additives?
- Smoke generator:
  - How effective is the smoke?
  - How is it supplied with fuel?
  - What fuel is used?
  - What maintenance is required?
  - Does the smoke contain any additives?

NBC Vehicles

List of subcategories.

- Reconnaissance vehicles.
- Area marking.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found.
- Data plate information.
- Power requirement.
- Inventory.
- Photographs.

Subcategory requirements.

- Reconnaissance vehicles:
  - Are they wheeled or tracked?
  - Are they equipped with overpressure?

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

- Reconnaissance vehicles (continued):
  - What chemical detectors are used?
  - What radiological detectors are used?
  - What miscellaneous NBC equipment is used?
- Area marking vehicles:
  - Are they wheeled or tracked?
  - Are they equipped with overpressure?
  - What chemical detectors are used?
  - What radiological detectors are used?
  - What type of marking sets are used?
  - What miscellaneous NBC equipment is used?

Medical Kits

List of subcategories.

- Personal kits.
- Medical kits.
- Specialized kits.

Main category requirements.

- Size.
- Weight.
- Manuals.
- Location found.
- Data plate information.
- Power requirement.
- Photographs.
- Inventory.

Subcategory requirements.

- Personal kits:
  - How and where are they carried?
  - What type of injuries and ailments can be treated?
- Medical kits:
  - How are they issued?
  - How and where are they carried?
  - What type of injuries and ailments can be treated?
- Specialized kits:
  - How are they issued?
  - How and where are they carried?
  - What type of injuries and ailments can be treated?

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Hospitals

List of subcategories.

- Aid stations.
- Mobile hospitals.
- Permanent hospitals.

Main category requirements.

- Size.
- Documents, manuals, and forms.
- Location found.
- Power requirements.
- Treatment capabilities.
- Personnel required to operate.
- Number of personnel that can be treated.
- Photographs.
- Inventory.
- Adjacent hospital activities (labs, clinics).
- At which level of command controlled.

Subcategory requirements.

- Aid stations:
  - Amount of time required to become operational.
  - Logistic support needed for movement.
  - Time required for evacuation.
- Mobile hospital:
  - Amount of time required to become operational.
  - Logistic support needed for movement.
- Permanent hospital:
  - Amount of time required to become operational.
  - Logistic support needed for movement.

Medical Vehicles

List of subcategories.

- Ambulances.
- Aircraft.

Main category requirements.

- Documents and manuals.
- Inventory.
- Photographs.
- Crew members required.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Main category requirements.

- Personnel transport capability.
- On-board treatment capability.
- On-board NBC protection capability.

Subcategory requirements.

- Ambulances:
  - Wheeled or tracked vehicles.
  - Type fuel used.

Messing

List of subcategories.

- Field utensils.
- Portable pots and pans.
- Portable immersion heater.
- Field rations.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location.
- Data plate information.
- Inventory.
- Photographs.

Subcategory requirements.

- Field utensils (material used).
- Portable pots and pans (types of material).
- Portable immersion heater (fuel used).

Field rations:

- Types.
- Preparation method.
- Number of servings per pack.

Camouflage and Concealment

List of subcategories.

- Camouflage netting.
- Camouflage screening.
- Camouflage clothing.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found.
- Data plate information.
- Inventory.
- Photographs.
- Colors.
- Pattern.
- Type of material used.
- Radar reflective (Y/N).
- Infrared reflective (Y/N).
- Serviceability and durability.

Subcategory requirements.

- Camouflage netting.
- Camouflage screening.
- Camouflage clothing.

Body Armor

List of subcategories.

- Body vest.
- Helmets.

Main category requirements.

- Size.
- Weight.
- Documents and manuals.
- Location found.
- Data plate information.
- Inventory.
- Photographs.
- Type of protection given.
- Type of material used.

Subcategory requirements.

- Body vests.
- Helmets.

Missiles, Rocket, and Munitions

List of subcategories.

- Artillery.
- Mortars.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

List of subcategories (continued):

- Bombs.
- Mines.
- Booby traps.
- Grenades.
- Missiles.
- Rockets.

Main category requirements.

- Size.
- Type and use.
- Filler.
- Fuze.
- Markings.
- Color code.
- System used in.

Subcategory requirements.

- Artillery and missiles:
  - Propellant and rocket motor.
  - Guidance.
- Mortars, grenades, and rockets (propellant).
- Mines (additional fuze wells).

Artillery

List of subcategories.

- Tube artillery.
- Antiaircraft guns.

Main category requirements.

- Towed or self-propelled:
  - Self-propelled (cab or turret, opened or closed).
  - Towed (type of prime mover).
- Caliber.
- Type of recoil (spring, hydraulic, pneumatic).
- Length of recoil movement.
- Type of elevation system (manual or power) and limit.
- Type of traverse system (manual or power) and limit.
- Muzzle brake and flash suppressor.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Subcategory requirements.

- Tube artillery:
  - Type of breech mechanism (sliding wedge).
  - Type of ammunition (fixed, semifixed, separate).
  - Rifled or smooth bore.
  - Bore evacuator.
  - Fire control (direct or indirect).
- Antiaircraft guns:
  - Single or multiple barrels.
  - Type of fire control.
  - Type of loading mechanism.
  - Type of firing mechanism (percussion, electric).
  - Gun drive system (manual, electric, mechanical).

Small Arms

List of subcategories.

- Pistols.
- Rifles.
- Machine guns.
- Cannons.

Main category requirements.

- Caliber.
- Type of feeding and quantity.
- Single shot or automatic.
- Smooth bore or rifled.
- Fixed or adjustable sights.
- Heavy or light weapon.
- Muzzle brake or flash suppressor.
- Type of ammunition used.
- Type of locking system.
- Gas or recoil operated.

Subcategory requirements.

- Pistols:
  - Revolver or semiautomatic.
  - Rimmed cartridge.
  - Last round stop.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Subcategory requirements (continued):

- Rifles:
  - Carbine, assault, or sniper.
  - Steel sights or scope.
  - What power scope.
  - Last round stop.
  - Fixed or removable bayonet.
  - Fires from open or closed bolt.
- Machine guns:
  - Heavy or light.
  - Vehicle mounted or handcarried.
  - Stock or spade grips.
  - Last round stop.
  - Fixed or adjustable bipod or tripod.
- Cannons:
  - Ground and antiaircraft capabilities.
  - Manual and electric fire.
  - Type of fire control.
  - Fires from open or closed bolt position.

Grenade Launchers

List of categories

- Handheld.
- Tripod mounted.
- Vehicle mounted.

Main category requirements.

- Caliber.
- Rifled or smooth bore.
- Method of loading.
- Firing method.
- Type of round.

Subcategory requirements.

- Handheld (attached to another weapon).
- Tripod mounted (crew served, number of members).
- Vehicle mounted (single or multitubed).

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Fire Control

List of subcategories.

- Off carriage.
- On carriage.

Main category requirements.

- Use (observation, target destination, aiming, range).
- Type (night vision, laser, optic).
- Style (periscope, telescope, stereoscope) and power.
- Reticle (type, quantity, stability).

Subcategory requirements.

- Off carriage:
  - Weight.
  - Tripod use.
  - Day or night use.
  - Durability.
- On carriage:
  - Location of mount.
  - Type of power for operation.

Recoilless Rifles

List of subcategories.

- Ground mounted.
- Vehicle mounted.
- Shoulder fired.

Main category requirements.

- Caliber.
- Smooth bore or rifled.
- Breech type.
- Type of firing mechanism.
- Spotting gun.
- Fire control.
- Type of round.

Subcategory requirements.

- Ground mounted:
  - Type of mount.
  - Elevation and traverse (methods and limits).
  - Crew served (number of members).

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Subcategory requirements (continued):

- Vehicle mounted:
  - Type of vehicle.
  - Elevation and traverse (methods and limits).
  - Type of mount (Can it also be used in ground role?).
  - Crew served (number of members).
- Shoulder fired:
  - Weight.
  - Pistol or grip.
  - Bipod.

Turret and Cupola Mounted Weapons

List of subcategories.

- Tanks.
- Infantry fighting vehicles.

Main category requirements.

- Type of vehicle.
- Location.
- Size.
- Weapons.
- Viewing and fire control.
- Method of operation (power, manual or stabilized).
- Ammunition storage (quantity, type, location).
- Attachments (lights, antennas, grenade projectors).

Subcategory requirements.

- Tanks:
  - Main gun:
    Caliber.
    Smooth bore or rifled.
    Bore evacuator and muzzle flash suppressor.
    Breech type.
    Recoil type.
    Elevation and traverse (method and limits).
    Firing mechanism.
    Ammunition types.
    Method of firing.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

- Tanks (continued):
  - Coaxial weapons:
    - Caliber.
    - Type.
    - Ammunition.
    - Method of firing.
  - Cupola:
    - Weapons.
    - Traverse and elevation (method and limits).
    - Fire control.
    - Method of firing.
  - Crew compartment:
    - Number of stations.
    - Firing ports.
- Infantry fighting vehicles:
  - Main guns:
    - Caliber.
    - Type.
    - Method of loading.
    - Method of firing.
    - Fire control.
    - Elevation and traverse (method and limits).
  - Coaxial weapons:
    - Caliber.
    - Type.
    - Method of loading.
    - Method of firing.
  - Crew compartment:
    - Number of stations.
    - Firing ports.
    - Ammunition storage (quantity and type)

Mortars

List of subcategories.

- Manpack.
- Towed.
- Self-propelled.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

Main category requirements.

- Caliber.
- Recoil type (if any).
- Traverse mechanism and limits.
- Elevation mechanism and limits.
- Type of firing mechanism.
- Type of ammunition (fixed or separate loading).
- Fire control.

Subcategory requirements.

- Manpack:
  - Mount type (base plate, tripod).
  - Number of crew members required and their mission (two for the tube, one for the base plate, three for the tripod).
  - Capable of mounting on a vehicle.
- Towed:
  - Prime mover.
  - Type of carriage (single or multiple axle).
- Self-propelled:
  - Type of vehicle.
  - Dismountable.

Figure D-8. Sample technical intelligence exploitation plan and category requirements format (continued).

STRUCTURES SURVEY FORMAT

1. Identification.
   a. Local and Official Name (from map study).
   b. General Location and Address.
   c. Map References. Identify by map series, sheet number, and edition.
   d. Coordinates. State in UTM.
   e. Additional Information. Indicate any peculiar information, date of original survey, and any updates if applicable.
2. Surrounding area.
   a. General Information.
      (1) General overview. Include aerial photograph(s).
      (2) Map references.
      (3) Additional information.
   b. Tactical Considerations.
      (1) Command posts (CPs). Include the following information:
         (a) Entrance(s) and approach routes.
         (b) Security, cover, and concealment.
         (c) Provisions for water, electricity, telephone, ventilation, rest rooms, adequate working space, and a secure area to install satellite communications (SATCOM) antennas.
         (d) Building and area recommended for the OPCEN, who owns the building, the address, the point of contact (POC), facilities available in the OPCEN area, and vehicle and foot approach routes to the building. (Ensure the CP is shown on the surrounding area sketch, and if possible, show photographs of the building and area.)
      (2) Surveillance positions. Include the following:
         (a) An overwatch of the area.
         (b) Concealed access routes to the CP and staging areas.
         (c) Secured and concealed accesses and/or entrances to the surveillance position.
         (d) Cover and concealment of the surveillance position from observation by personnel located on the site.
         (e) Provisions for water, electricity, and rest room facilities.
         (f) The location of the surveillance position on the surrounding area sketch. (Show photographs of the building in which the surveillance position is located, the surveillance position

Figure D-9. Sample structures survey format.

in the building, the view from the surveillance position to the site, and the view from the site to the surveillance position.)

(g) A description of the following:

1. Type of building.
2. Number of stories.
3. Location of surveillance position in relation to the site.
4. The area to be used by the observer.
5. Who owns the building, address, POC(s), and their telephone numbers.
6. Access routes to the area.

(3) Staging areas. Include the following:

(a) Whether the structure has a basement or other large area concealed from outside view.

(b) If the staging area is in the vicinity of the site, preferably in the surrounding area.

(c) Suitability for holding 30 to 40 men for 2 to 3 days.

(d) Provisions for water, electricity, and rest rooms available, if possible.

(e) Whether routes to the CP are concealed from observation by personnel located on the site.

(f) Concealment of accesses (for example, underground parking lot).

(g) The location of the staging area in relationship to the site, who owns the building, POC for access and his telephone number, recommended approaches to the area, and recommended entrances. (Show the location of the staging area on the surrounding area sketch and photographs of the building and the area.)

(4) Recommended approaches. Include the following:

(a) Main direction from the staging area to the site and surveillance positions.

(b) Whether approach is by air, land, or water.

(c) Whether it is by vehicle or foot.

(d) Any unusual circumstances about the approach (for example, an approach over rooftops of surrounding buildings, facilities such as banks located near the approach that may have 24-hour guards).

Figure D-9. Sample structures survey format (continued).

(e) Blind or unsecure spots on the approaches.

(f) If possible, photographs of the route from the staging area to the site along the recommended approach.

(5) Sanctuaries. Include the following information:

(a) Friendly government embassies, churches, and American facilities or residences in the area.

(b) The building and the area to be used as the sanctuary.

(c) Who owns the building, the address, the POC and telephone number(s), location in relation to the site, and what the facility is normally used for.

(d) Location of the sanctuary in relation to helicopter landing zones (HLZs) and evacuation routes.

(e) Location of the structure on the surrounding area sketch. (Show photographs of the building and, if possible, of the area to be used as sanctuary.)

(6) Obstacles and/or danger areas. Include the following information:

(a) Vegetation and terrain surrounding the site.

(b) Open areas (for example, large avenues adjacent to the site).

(c) Locations of guarded banks or other guarded facilities, hostile country embassies, and threat group offices.

(d) High crime areas and the most common type of criminal occurrence in these areas.

(e) Roadways or avenues recommended for approaches that are affected by rush hour traffic.

(f) Checkpoints, curfews, police or security patrols, universities, construction areas, police or military installations.

(g) Exceptionally well illuminated areas around the site.

3. Grounds description.

a. General Description. Always orient the direction of the survey to main directions. Pay particular attention to basic locations, type of construction, distances from perimeter barriers to principal structures and then structures of a secondary nature to the principal structures.

b. Perimeter Barrier. Total information coverage is required. Emphasize heights, widths, and thicknesses. Zero in on weak spots and describe them in detail.

c. Entrances to Grounds. Examine points of normal or prepared access, style of construction, security and/or locking devices, closed-circuit televisions (CCTVs), and guards.

d. Structures. Include any additional structures located on the grounds.

Figure D-9. Sample structures survey format (continued).

e. Terrain and Vegetation. Provide a very simple description (for example, height and type of trees).

f. Additional Information. Include possible routes of access and masking effect of vegetation.

4. Building description.

a. Exterior. Give a general description to include basic style of construction. Make reference to aerial photographs, if available.

b. Entrances to Building. Give a detailed description including names of entrances, if applicable.

(1) Main entrances. Working from outside to inside, describe the entrance and any entrance procedures, if applicable. Describe hinges from the top down.

(2) Other entrances. Describe the same as above.

(3) Emergency entrances and exits. Describe the same as above.

(4) Additional information. Include grates, air conditioning ducts, fans, and trap doors.

c. Interior Description of Building.

(1) General description.

(2) Floor plans. Refer to attached floor plans and floor plan sketches.

(3) Floors. Include type of construction of the floors from the basement up.

(4) Corridors. State width, height, type of lighting, type of floor covering, depths of doorways, and general information.

(5) Stairways. Describe by name if possible, and describe the locations of landings and banisters. Give the number of stairs.

(6) Elevators. Include mechanism, escape hatch, and other contents of the elevator (off the data plate) including any limitations of the elevator (for example, that it does not service the top floor).

(7) Doors and locks. Refer to a specific industry or professional standard door/lock/key chart available to all participating organizations.

(8) Windows and locks. Describe standard type(s) for the specific structure and any exceptions.

(9) Physical barriers. Describe any barrier system that will be used during an emergency.

(10) Hardened areas. Describe in detail.

Figure D-9. Sample structures survey format (continued).

(11) Weak points. Describe in detail.

(12) Additional information. Describe in detail.

d. Roof.

(1) General description. List antennas, elevator rooms, and type of construction.

(2) Entrances and exits. Describe in detail, with emphasis on areas of weak construction.

(3) Fire escapes and ladders. Describe in detail.

4. Common systems.

a. Security.

(1) Personnel.

(a) Marine security guards. Give the numbers and types of weapons carried.

(b) Security detail and/or bodyguard. Describe the same as above.

(c) Contract watchmen. Give the numbers, types of weapons, and times of shift changes.

(d) National policemen. Give the numbers and affiliation with the facility.

(2) Total security equipment. Include a total inventory of all security equipment.

(3) Sensors and alarms.

(a) Location outside.

(b) Location inside.

b. Communications.

c. Organic Transportation.

d. Medical Equipment.

e. Power.

(1) Explain primary, normal system (for example, source and shutoff data).

(2) Explain backup and emergency system(s) (for example, source, shutoff data, and duration capability).

(3) Provide additional information.

f. Air Conditioning and Ventilation. Explain the air conditioning system, with special emphasis on vents and air intakes.

g. Sewage and Drainage. Explain the sewage system that services the structure with a special emphasis on access to the structure, if any.

h. Additional Information.

Figure D-9. Sample structures survey format (continued).

5. Personnel structure.

a. Staffing Pattern.

b. Key Personality Data.

c. Additional Information.

(1) Draw north arrows on the photographs and annotate items of importance on them. Do not annotate on a photograph an item indicated on the legend and/or label, unless necessary.

(2) Assemble finished product in the following order:

(a) Table of contents.

(b) Narrative description.

(c) Surrounding area sketch.

(d) Photograph and/or slide index.

(e) Photographs with labels, north arrows and annotations.

(f) Slides.

(3) Have another person check for accuracy.

NOTE: Attached as an enclosure should be the door/lock/key reference information. The standard format for the door system should be very simple and not require a great deal of time either to collect information against or to produce a survey from. The preparer should specifically—

1. List all doors.

2. Note whether they are standard or not, giving a definition of what a "standard door" for that particular structure is.

3. Describe any door that is not standard.

Figure D-9. Sample structures survey format (continued).

BEACH SURVEY FORMAT

1. General information. Include the following:
   a. The date(s) the survey was conducted.
   b. The date the report was prepared.
   c. The code identity of the unit conducting the survey.
   d. The code identity and location of the beach surveyed. Also include the following:
      (1) Reference maps or charts used.
      (2) Code designation or name of the beach.
      (3) Coordinates of the beach flanks.
      (4) Landmarks used for identification and their position relative to the center of the beach (as seen from seaward).
   e. The datum plane used to determine the shoreline.
   f. A brief description of the conditions under which the survey was conducted to include weather, visibility, and threat interference.
   g. A list of items appended to the report.
2. Beach description. Provide detailed description of the beach, including:
   a. Beach length and configuration.
   b. Usable beach length.
   c. Beach interruptions and obstacles.
   d. Subsurface hazards (for example, rocks, shipwrecks, dragon's teeth, and mines).
   e. Type of coastline.
   f. Foreshore description.
      (1) Width.
      (2) Gradient.
      (3) Composition.
   g. Backshore description.
      (1) Width.
      (2) Gradient.
      (3) Composition.
      (4) Vegetation.
      (5) Exits.
      (6) Trafficability.

Figure D-10. Sample beach survey format.

3. Threat activity. Describe observed threat or nonbelligerent third party situation. Include a precise description of all man-made objects on the beach, whether or not obviously erected for beach defense. Do not limit the focus to the beach itself, but cover all activities observed.

NOTE: Sketches, photographs, and videotapes are normally attached to the beach survey. TACBEREPs and SURFREPs may also be attached.

Figure D-10. Sample beach survey format (continued).

HYDROGRAPHIC SURVEY FORMAT

1. General information. Include the following:
   a. The date(s) the survey was conducted.
   b. The date the report was prepared.
   c. The code identity and mission of the unit conducting the survey.
   d. The code identity and location of the area surveyed. Also include the following:
      (1) Reference maps or charts used.
      (2) Code designation or name of the beach.
      (3) Coordinates of the beach flanks.
      (4) Landmarks used for identification and their position relative to the center of the beach.
   e. The datum plane used to determine the shoreline.
   f. A brief description of the conditions under which the survey was conducted to include weather, visibility, and threat interference.
   g. A list of items appended to the report.
2. Hydrographic description.
   a. Provide a detailed hydrographic description of the area, including—
      (1) Beach length and configuration.
      (2) Usable beach length.
      (3) Beach interruptions and obstacles.
      (4) Type of backshore.
      (5) Surf characteristics.

Figure D-11. Sample hydrographic survey format.

(6) Inshore currents.
(7) Tidal ranges and times.
(8) Nearshore description.
(a) Distance from the shoreline to the 1-, 2-, and 3-fathom curves.
(b) Gradient.
(c) Bottom composition.
(d) Reefs, bars, shoals, or seaweed.
(e) Other obstacles.
(9) Foreshore description.
(a) Width.
(b) Gradient.
(c) Composition.
(d) Runnels (rivulets), cusps (points), or scarps (steep slopes or cliffs).
(e) Other obstacles.

3. Threat activity. Describe observed threat or nonbelligerent third party situation. Include a precise description of all man-made objects in the area surveyed, whether or not obviously erected for defense. Do not limit the focus to the beach itself, but cover all activities observed.

4. Hydrographic sketch (attached). Provide a graphic presentation of the nearshore and foreshore areas. (It is a 1:1,000 or 1:2,500 scale drawing that shows the shoreline; the 1-, 2-, and 3-fathom curves; the foreshore; obstacles; cultural features; beach flanks; and beach interruptions as seen from above). Depict the nearshore and foreshore gradients by showing three cross sections taken at the beach center and in the middle of the left and right sections of the beach. (The vertical scale of the cross sections is usually larger than the horizontal scale of the cross sections). All soundings by the survey party are shown on the sketch.

NOTE: A beach survey, TACBEREP, SURFREP and/or DELTREP can be attached to this report. See Chapter 4.

Figure D-11. Sample hydrographic survey format (continued).

DEBRIEFING FORMAT

NOTE: This format follows the postmission report (Annex L of SODARs) and is used as a guide for debriefing SFODs. Refer to the SODARs procedural handbook for format instructions. SODARS is available through USSOCOM's SOCRATES that is available to units within the USSOCOM.

(CLASSIFICATION)

1. ( ) Mission data:
   a. Mission number:
   b. Specific type mission:
   c. Unit:
   d. Exercise/operation name:
2. ( ) Countries:
3. ( ) Unified command/higher headquarters:
4. ( ) Summary statement of mission:
5. ( ) Date of deployment:
6. ( ) Date of return:
7. ( ) Maps used: (series, sheet, edition, classification, scale)
8. ( ) Task:
9. ( ) Size and composition of SFOD for mission:
10. ( ) Mission members: (Name, position, and duty)
11. ( ) Time of departure:
12. ( ) Time of return:
13. ( ) Ingress/egress:
14. ( ) Terrain:
15. ( ) Enemy:
16. ( ) Map corrections:
17. ( ) Results of enemy encounters:
18. ( ) Actions at the target:
19. ( ) Communications:

Figure D-12. Sample debriefing format.

20.( ) Weapons:

21.( ) Demolitions:

22.( ) Medical information:

23.( ) Lessons learned:

24.( ) Were U.S. human rights policies adhered to?

25.( ) Miscellaneous information:

26.( ) Authentication data:

a. Reviewed by mission support unit (MSU)____ Forwarded to mission support center (MSC)____

b. Reviewed by MSC____ Forwarded to component (DTG)____

c. Reviewed by component____ (DTG)____

27.( ) Report incorporated into annex____

a. ( ) DTG:

b. ( ) POC:

(CLASSIFICATION)

Figure D-12. Sample debriefing format (continued).

The observation log is a record of what was seen and is not an analysis. Fill out the log using the key word "SALUTE" for threat force activity and "OCOKA" for terrain. When using these key words to make log entries, do not waste time on generalities but be very specific (for example, exact number of troops, exact location, exact disposition). The log is always used in conjunction with a field sketch, and the field sketch supports data entered into the log. Also keep supplemental notes. The log is an important source of operational information and, at a minimum, should include—

- Call sign of the observer or SFOD.
- Observer or site code location.
- Visibility/night.
- Time of observation (DTG group in local time).
- Grid coordinates or reference of observation.
- Event or activity observed.
- Action taken.

SKETCHING, MAPPING, AND PHOTOGRAPHY

The goal of SR is to produce useful information. Sketches, maps, and photography techniques aid in the storage, production, and transmission of this information.

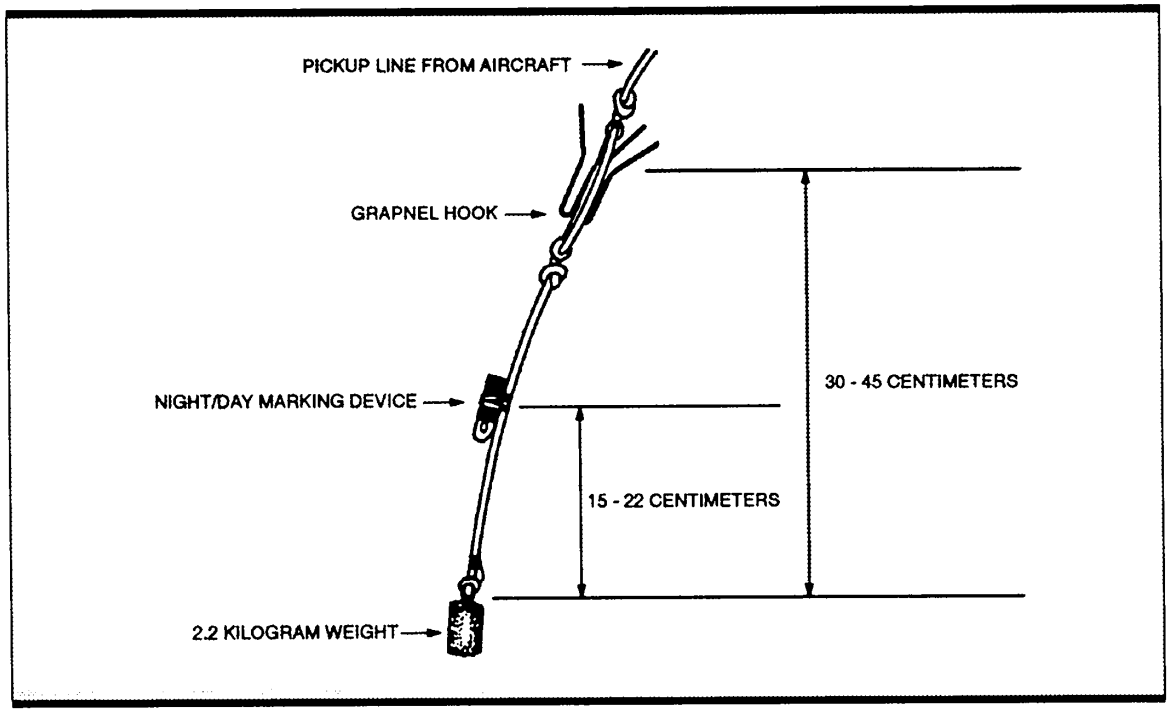


Figure C-4. Aircraft pickup line assembly.

Month: NOV 90
DTG

LOCATION: JERICHO 3
OBSERVERS: TM RED/TM BLUE

ENTRY	FROM	TO	WHAT NOTED AND WHERE	ACTION TAKEN/VISIBILITY
1	260001		OP activated by Team Blue.	Logged/Low ovrcst 500m
2	260430	260550	RP 3, right 50 M, 3 men burying sacks.	Obsrvd, photo'd/Clear 5 mi
3	260930		RP 2 to RP 7, 1 semitrailer passed on Rte 101.	Logged/Clear 10 mi
4	261340	261345	RP 4, 200 m right, military UH-1 flying low level.	Logged/Clear 5 mi
5	261713		RP 7 to RP 2, two cars passed on Rte 101, appeared at RP 3, 10-20 m right.	Obsrvd, photo'd/Lt drizzle
6	261800		Shift change. OP relieved by Team Red.	Logged/Rain 2 mi
7	270530	270640	RP 1, 10 m right, lone man on bicycle placing soft drink can on side of road.	Obsrvd, phot'd/Fog 300 m
8	270600		Shift change. OP relieved by Team Blue.	Logged/Fog 400 m
9	271045	271120	RP 5, 50 m left, two men moving SW toward road.	Obsrvd, logged/Fog 1 mi
10	271315		RP 1, 150 m NNE, two men sitting in bush, facing road.	Photo'd, logged/Clear 10 mi
11	271430		RP 2, 25 m left, pickup truck pulled off road on south side.	Infrmd tm ldr, logged/clear
12	271445	271520	RP 2, right 25 m, lone occupant of truck walking SE along S side of road.	Photo'd, logged/Clr 15 mi
13	271520	271530	RP 1, 10 m right, truck occupant picking up soft drink can, returning on foot to truck.	Photographed, logged, infrmd Tm ldr/low ovrcst
14	271530	271540	RP 2, 25 m left, truck U-turns, departs NW Rte 101	Logged/Mist 1 mi

Figure C-5. Sample observation log.

Sketching

Always use a sketch as a backup. Prepare panoramic and topographic sketches of the targets. These sketches are excellent supplemental or backup material for written logs. Accuracy, detail, and scale are vitally important. Graph paper, blueprints, fire plans, photographs, and other aids may be used in the preparation of the sketch. Ensure all sketches are in proportion, use correct terminology (for example, types of windows), use standard terminology and symbols, and have a north arrow.

Panoramic Sketching. A panoramic sketch depicts terrain in elevation and perspective as seen from the point of observation. It can also be a sketch of a specific building, item of equipment, or other object of interest. One method of panoramic sketching is to establish a scale on the paper on which the sketch is to be drawn, draw the horizon of the terrain or outline of the object, and then fill in the details. When drawing terrain, focus on observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach (OCOKA). When making the sketch, carefully depict fields of observation and fire from the target outward as well as from suitable points facing in toward the target. When drawing an object, such as a building or item of equipment, focus on such factors as windows, doors, intakes, obstacles, barriers. When sketching personnel, focus on the size, activity, location, unit, time, and equipment (SALUTE) factors. When adding details to a sketch, use a system to ensure thoroughness. For example, when sketching individuals, draw the outline of the individual and then fill in details from top to bottom, left to right.

Topographic Sketching (Mapping). A topographic sketch is an overhead representation similar to a map. It can be of a geographic area or it can be a floor plan of a building. One method of topographic sketching is to establish a scale on the paper on which the sketch is to be drawn, draw a grid and magnetic north arrow, establish grid lines, draw the outline of the building and/or other objects of interest in the sector, and then fill in the details. Accuracy, detail, and scale are vitally important. When drawing terrain, focus on the OCOKA factors. When drawing a building or facility (for example, a weapons emplacement or base) focus on such factors as doors, windows, composition and thickness of walls, layout of obstacles and barriers. Where human activity is represented in the text, the focus is on the SALUTE factors. When adding details to a sketch, use a system to ensure thoroughness, for example, top to bottom and left to right.

Photography

A well-taken picture is truly worth a thousand words. In the conduct of SR, SF photography is often an invaluable skill.

IMINT Collection. IMINT collection is an extremely important task for an SFOD A in its operational area. The SFOD can collect, confirm, or reinforce technical information through on-the-ground photographic surveillance, which cannot be done by more technical means. Consider the IMINT principles discussed in the following paragraphs.

Practice makes perfect. Consistently practice photographic techniques. Rehearse these techniques under the light and weather conditions that are expected in the operational area. Lack of adequate practice could result in overexpose, underexposure, or wasted shots, which may cause mission failure.

An unloaded camera shoots blanks. Always keep the camera loaded and readily accessible. Before departure, check the camera to ensure it is loaded with the proper film. Immediately after exposing a roll of film, reload the camera.

Film is cheap. Carry several rolls of film of various capabilities. When lighting conditions are questionable, bracket exposures. It is better to have too many photographs of the target than to be missing the one critical photograph. When in doubt, shoot the picture.

NOTE: *Never photograph SFOD members on a mission. If threat forces capture film with images of the SFOD on it, they can determine the SFOD's strength and capabilities.*

When taking photographs of more than one target on a mission, do not carry the film of the previous target(s) to the next target. Cache previously exposed film. Pick up the exposed film when it leaves the AO. The capture of multiple rolls of film with pictures of several targets could seriously compromise U.S. intentions in the area.

Always photograph an object of identifiable size (such as a cartridge or a military pen) with the subject to help identify its dimensions. If operating in an urban environment or other area where military items should not be carried, an indigenous coin or a 15-centimeter plastic or wood ruler may suffice to show size.

Types of Photography. There are five types of special purpose photography applicable to SR missions.

Identification photography deals with photographing personnel or groups of personnel to identify and record the identity of the subject(s). The subject may or may not be aware that he is being photographed. Examples of identification photography include—

- Photographing indigenous personnel for pay and/or service records.
- Photographing threat personnel, dead or alive, to obtain OB information.
- Clandestinely photographing drug traffickers in support of HN counterdrug (CD) operations.

Documentation photography is used to record printed material or other photographs. Examples of documentation photography include—

- Photographing base camp records to be cached.
- Photographing captured or acquired maps and overlays.
- Photographing documents that would compromise a sensitive operation if they were removed.

Technical photography is the photographing of equipment or mechanical or electrical items so that the photograph may be analyzed in lieu of the actual item. Include a measurement scale in technical photographs. A 15-centimeter ruler is an excellent scale for most small items such as individual weapons and radios. Expedient scales such as currency, a like item of U.S. manufacture, or a known round of ammunition may be used. Examples of technical photography include—

- Photographing an item of equipment that is too large for exfiltration.
- Making a photographic inventory record.
- Photographing a piece of equipment that would compromise a sensitive operation if removed.

Surveillance photography is an advanced technique used for obtaining information about an individual or an installation under a full range of threat, weather,

and terrain conditions. See AR 381-10 and FMs 34-60A and 31-26(U) for detailed information about personnel surveillance. Surveillance photography implies that the target is unaware it is being photographed. Surveillance photography may require the use of spotting scopes, telephoto lenses, and binoculars. Take photographs of stationary subjects at night through a combination of American Standards Association (ASA) compensation and "push processing."

Photography that is purely of the identification, documentation, technical, or surveillance type is seldom used. Most SR photography combines some principles from all of them. For example, photography of an industrial site for technical evaluation may require the following types of photography:

- ***Surveillance*** —to provide an overview of the target area, its perimeter, avenues of approach, access, egress, fields of fire as seen from particular vantage points.
- ***Identification*** —to identify key individuals.
- ***Documentation*** —to obtain copies of access documents, duty rosters, wiring diagrams, and flow charts.
- ***Technical*** —to picture circuit boards, pipe fittings, switch panels, or gears.

Equipment. Collect IMINT with the KS-99 series camera system, the electronic filmless camera system, and various off-the-shelf still and motion photographic systems.

The KS-99 series camera system is based on a single-lens reflex (SLR) 35-mm self-contained, portable, hand-operated camera. The camera can be used to photograph most still and moving subjects under various lighting conditions. It is used mainly for black and white or color photography under conditions where small, readily portable equipment is desired and small picture format may be used. The KS-99 series cameras may vary in body type. Refer to the manufacturer's handbook for specific information and STP31-18F4-SM-TG for further information and functions of the KS-99.

A wide variety of off-the-shelf, small, lightweight, battery-operated, hand-held videocamera systems can be used. These systems include a camera, recorder, and lighting equipment. Some of these cameras are comparable in size and weight to an SLR camera body with a lens. All offer the advantage of being able to take motion pictures with sound. Most modem systems also can record the date-time group (DTG) on the film as the pictures are being taken, which aids in the accurate timing of events or activities being recorded. Disadvantages of these systems are that they do not perform well in below-freezing environments and their acuity is not as great as with a 35-mm camera system under most circumstances. They also generally do not perform as well in low light conditions without the use of NVD type lenses. More advanced technology can also be used. The electronic filmless camera system (EFCS) records still images and motion pictures electronically instead of using the standard photographic process. The EFCS stores information and converts it to a digital data stream for transmission via secure or nonsecure radio and/or satellite on command. The primary advantage of the EFCS over 35-mm and videotape photography is its NRT image transmission capability. The most important limiting factor of the EFCS is light conditions. Other limitations include transmission times, size of the equipment, weather, and other factors that would limit normal 35-mm photography.

Photographic Techniques. Techniques for taking a useful photograph depend on many considerations. Photography can be planned as an operation using METT-T.

Sequence. When taking a series of photographs of a complex item or area, use a logical sequence. Normally, Americans view subjects from left to right and from top to bottom. Also, when photographing an installation, it is good to go from the broad to the narrow, or from outside to inside, along the same or a similar path that would be viewed by other forces. When multiple, closely sequenced moving or still photographs are taken along such a path, as in moving along streets and inside buildings, the effect of "surrogate travel" can be created. Photograph technical items from the general to the specific and from the whole to individual pieces.

Subjects. Generally, threat force activity has the most intelligence value in SR operations. Terrain and weather information can also be important. What will or will not be photographed is largely determined by PIR, IR, SIR, and METT-T.

You may find yourself photographing the following types of subjects:

- Installations.
- Equipment.
- Caches.
- Roads.
- Communications and power transmission lines.
- Personnel.
- Terrain.
- Moving subjects.

Installations include military fortifications, terrorist safe houses, and drug laboratories. Photograph installations to show location, security, dimensions, construction, accesses, and other features. Photograph the entire installation using a wide-angle lens or by using panoramic photography. Note on the photo log the direction (in degrees, 3 digits) in which the photo was taken and the location from which it was taken. Overlap panoramic frames to prevent the loss of any details. Then join these photographs to create a photomosaic. Shoot key emplacements using a telephoto lens, a spotting scope, or binoculars.

Shoot equipment, including weapons systems, vehicles, industrial machinery, and ammunition stocks to show dimensions, capabilities, identifying markings, and other features. Place small equipment on a flat surface and photograph it from above. Photograph large items as they are found. Use technical photography techniques. When possible, first photograph the subject in its original position to establish place. Next, if time permits, photograph the item whole. Then disassemble the item and photograph the components in relation to one another. Finally, photograph each piece. If the item is to be retrieved, reassemble the item.

Shoot caches to record their location and contents. Photograph the cache site as it is approached to establish place. If time permits, use technical photography to photograph the containers and their contents, paying particular attention to any markings.

Shoot roads, trails, vehicle tracks, and any paths for movement from each direction (noted on photo log) to establish place. Use technical photography to photograph details such as road surface, shoulder, footprints, or vehicle tracks.

Shoot all poles, wires, or cables found. Photograph the cleared right-of-way in both directions and the adjacent terrain to determine place. Also shoot key items such as insulators, transformers, and cable supports, using technical photography if possible. Use a telephoto lens to obtain close-ups of those components situated above the ground.

Unless a telephoto lens is used, photographs of personnel at ranges in excess of 100 meters do not show enough detail to be useful for identification purposes. In most SR situations, close-up photographs are difficult (but not impossible) to take. Take most identification photographs at intermediate ranges with a telephoto lens. When gathering information on personnel in general, concentrate on identifiable uniform or clothing items. When the subject is a specific individual or group of individuals, concentrate on facial features or any other identifiable features instead of clothing and equipment. When conducting surveillance, concentrate on behavior of those located near the target.

You may be tasked to photograph representative terrain in an AA or terrain in and around a specific target. When shooting terrain, concentrate on the OCOKA factors.

Under favorable light conditions, capture moving subjects with a fast shutter speed and stop action. Under low light, shoot moving subjects with longer shutter speeds by "panning" the camera.

Taking the photograph. After a general plan for taking the required photographs is established, it is time to push the shutter. Bear the following in mind when taking photographs:

- Camera support.
- Composition.
- Focus.
- Exposure.

Hold the camera as steady as possible. With slow shutter speeds or during telephoto photography, use a tripod or field-expedient steadying device such as a rock or a tree. To determine the slowest shutter speed for hand-held cameras, use the reciprocal of the lens focal length, for example, a 50-mm lens becomes 1/50. Since there is no 1/50 shutter speed, round up to 1/60. When taking photographs from aerial platforms, however, do not brace the camera against the aircraft frame. The speed and vibrations of the aircraft create movement of the camera in relation to the target and blur the image on the film, even with a fast shutter speed.

Center the subject in the viewfinder to assure maximum detail is obtained. If the subject does not fit the frame, switch to a wide-angle lens or use panoramic photography. The size of the image in the viewfinder is not proportionate to a 20- by 25-centimeter enlargement. The image should not be crowded horizontally when the camera is held normally or approximately 15 percent of the image will be lost when an enlargement is made.

Get a sharp image in the viewfinder before exposing the film. Focusing aids located in the viewfinder are used for proper focus. Because of possible image deterioration, do not attempt to shoot through glass or plastic windows. Under low light conditions when the target cannot be seen in the viewfinder, preset the estimated range based on the distance scale of the focusing ring.

Use the light meter in the camera to determine the correct exposure. Follow instructions for the camera and the film to ensure the film is neither overexposed nor underexposed. The exposure is either aperture or shutter priority. Most SR photography is aperture priority, emphasizing the maximum depth of field. Shutter priority is used to obtain photographs of moving targets. In night photography, the degree of illumination (moonlight, ambient man-made light) determines aperture and shutter settings. Take test photographs during isolation, under the same or similar conditions expected during the mission (for example, moon phases, risings, and settings). If more than one camera is available and/or multiple photographs will be taken, "bracket" the aperture and shutter settings to increase the probability of good, clear photographs.

Making a record. Document all photographs on a photography log. This record greatly enhances the information value of the photographs. Document photographs with a log shown in Figure C-6. Record the following information in the log as soon as the photograph is taken, or as soon as practical thereafter

- Type of camera (make and model).
- Number of the exposure.
- Target or subject designation.
- Azimuth and/or distance from the photographer to the target.
- DTG of photograph.
- F/number.
- Shutter speed.
- Lens used.
- Remarks, including pertinent information such as universal transverse mercator (UTM) grid and/or geographic coordinates, direction, and number of the target.
- Roll number of the film (for example, 1 of 2).
- Type of film (for example Tri-X Pan).
- ASA number of the film and the ASA number at which it was exposed (for example, ASA 400 ei 1600 ["ei" being the abbreviation of exposure index on the camera]).

Field development. Where possible, bring a compact field development kit to the surveillance site. Such kits for 35-mm color slide film are particularly compact and quick. The advantage of having such a kit is that you can quickly check the results of your work and, if the subject is still in sight, take more photographs as needed. Field development may also be done in the ORP and/or MSS, from where, if not compromised, you may return to the target area if the photographs taken do not meet mission requirements. Film taken in the field and field-developed photographs can also be evacuated via aerial message pickup, if the situation dictates.

SURVEILLANCE TECHNIQUES

Surveillance techniques include the systematic observation of aerospace, surface or subsurface areas, places, persons, or things. Visual, aural, electronic, photographic, or other means are used for these surveillance techniques.

PHOTOGRAPHY LOG

EXP.	SUBJECT OF PHOTO	DIST/AZM TO TGT	Nov 92 DTG (LOCAL)	F/STOP	SHUTTER SPEED	LENS	REMARKS
1	Main Entrance	200m - 210°	191015R	16	500	200m	210mm
2	Secondary Ent.	150m - 85°	191017R	16	250	200m	210mm
3	W. Side of Bldg.	200m - 50°	191019R	16	250	200m	70mm
4	N. Side of Bldg.	25m - 100°	191030R	8	250	200m	70mm - Rear Ent.
5	E Side of Bldg.	75m - 200°	191119R	16	250	200m	70mm - Comm. Dish
6	Comm. Dishes	60m - 175°	191120R	16	250	200m	185mm
7	N.E. Ent.	10m - 250°	191129R	8	280	200m	70mm
8	N.E. Ent.	.5m - 240°	191132R	1	250	200m	MACRO of lock
9	W. Ent.	100m - 70°	191145R	8	125	50mm	
23	Jason Russell	5m	201145R	5.6	60	50mm	I.D. w/Flash
24	David Cypert	5m	201150R	5.6	60	50mm	I.D. w/Flash

ROLL NUMBER: 4 of 5 | FILM TYPE: Tri-X | ASA: 400

CAMERA: KS99 | PHOTOGRAPHER: Louis

Figure C-6. Sample photography log.

Routine

Operation of an observation or surveillance site can produce very important and high-quality information, but it is normally extremely boring work. Even under best conditions, for example, the concentration of the average observer looking at the same piece of ground seldom lasts more than 30 minutes. If two observers are on duty for 2 hours, they alternate as observers every 15 minutes. The man who is not observing acts as a sentry and observes the area around the site to prevent surprise attack or discovery.

Viewing Techniques

When viewing from ail urban and rural buildings, avoid windows and door openings that attract the attention of threat observers and snipers. Depending on the situation and your imagination, a wide variety of viewing techniques may be used against an urban target.

Window (Any Opening) Viewing. Where a window (opening) is being used for viewing a target, lower the risk of compromise by erecting a fiat black background screen just inside the windows and wearing the same flat black clothing. If the

screen is properly erected and you remain still, you will blend in with the normal shadow inside the window. This technique works better in a window with glass. Where the site is overt, as in some counterinsurgency (COIN) operations, you can cover the viewing ports with black Hessian screen that allows movement and observation without giving a sniper a clear target. To lower the vulnerability to grenade attack, cover the viewing ports with screens. Avoid grenade attacks by using the upper floors for the site.

Acoustic and Laser Monitoring. Where the target is a person or persons on the other side of a pane of glass, you may be able to hear and record conversations with off-the-shelf directional sound amplification devices and/or laser eavesdroppers. In either case, the window acts as a modulator, vibrating in sympathy with the speech in the room. With sound amplification equipment, you can retrieve audible sounds from the glass surface. With laser eavesdropping, a laser beam is reflected off the window to a receiver, which electronically converts the pulses made by the window to audible speech. Either technique may be defeated by thick curtains and recorded background chatter or music directed toward the window. These items are available to both friend and foe alike. Take countermeasures when talking or conducting meetings in a possible threat area. Simple steps, such as holding the conversations in a low voice, hinder threat force monitoring.

Fixed Site Equipment

You must have several items with you in the site: personal weapon, individual NBC protective equipment, optical instruments for observation, compass, watch, map, observation log, communications equipment, and all the food and water you will need for the duration of the mission (unless resupply is feasible). The principal documents are a diagram of reference points and the observation log. The diagram of reference points is similar to a range card, and in fact, a DA Form 5517-R can be adapted to this purpose. Figure C-7 is an example of a diagram of reference points. On the diagram, depict reference points by sketching those terrain features that correspond to the reference points in question. Other terrain features (for example, hills, woods, rivers) are shown by conventional topographic symbols, while the point of observation is shown by a tactical symbol. See FM 101-5-1. The observation log is a written record of what was observed, where it was observed, and when the observation took place. Use this log in conjunction with other observer notes, sketches, and photographs. See Page C-6 for a discussion of SFOD record-making techniques and procedures.

Organization of Surveillance Sectors

Have the SFOD leader ensure the entire sector is covered. Review reporting procedures with the observer prior to occupation of the observation site. Ensure that stable and reliable communications means exist between the observation site and the communications site, patrol base, or main body. In the observation site, conduct observation according to a given sequence.

The observer sector is divided into near, far, and middle zones, designated by arbitrary lines on the basis of terrain features, illumination, and/or reference points. The near zone includes the terrain area within which small targets can be seen with the naked eye. The middle zone is within the limits of visibility of prominent terrain features. The far zone takes in the rest of the expanse to the limits of visibility with optical instruments. When dividing an observation sector

into zones, at the same time determine the dead ground, i.e., unobservable sectors of terrain, and give them special attention since these sectors can be used by the threat force as concealed approaches.

As a rule, first inspect the terrain with the naked eye and then, using the optical instruments, inspect those areas in which threat targets may be positioned. Observation with an instrument alternates with observation with the naked eye to alleviate the potential for eye fatigue.

Look for indicators, spot threat targets and activities, and determine their locations. Record positions of targets in relation to known reference points. If possible, note the estimated coordinates of the targets. Use range-finding instruments and a compass to pinpoint target locations through modified resection.

During mission execution, you will need to be relieved. At the time of relief, inform the relieving observer of the mission assigned. Give him the observation sector on the terrain and to what he is to give special attention. Also give him the reference points, all targets discovered, the disposition of any friendly units in the area, and the location and nature of threat activity in the area. Report on the relief to the SFOD leader.

NOTE: *Observation of the target must not be interrupted while the observers are changing shifts.*

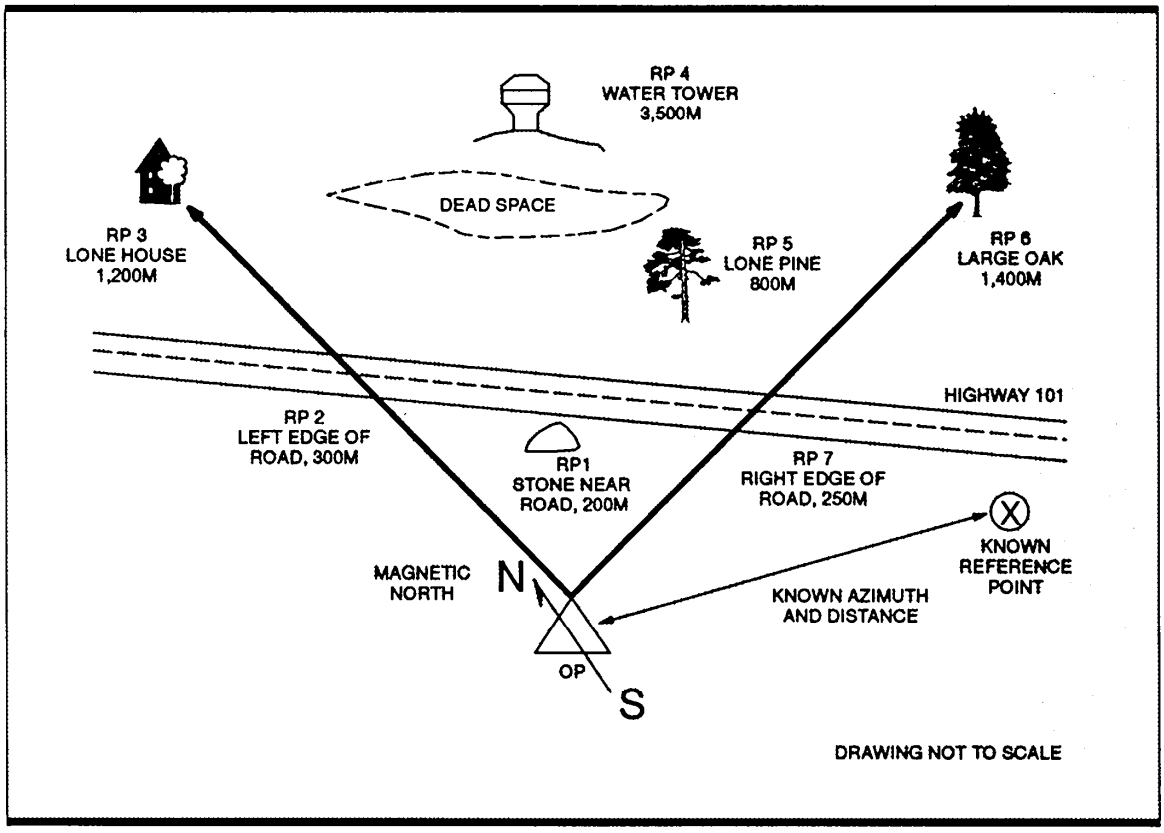


Figure C-7. Reference point diagram.

Night Observation

Darkness limits visibility, changes the outlines of objects, and distorts perceptions of distance. Dark objects seem farther away, while light ones seem closer. Therefore, orientation on the terrain and the detection and identification of objects is more difficult at night than during the day. Night observation is conducted with the naked eye and, for particular applications, night vision devices. Plan and organize night observation during the daylight period before the onset of darkness. Have the SFOD leader verify the location of observation sites and the readiness of the observers for night work.

Techniques. Military operations are often conducted during the hours of darkness. Some techniques for night observation are described below.

Dark adaptation. The exposure to light directly affects night vision. Repeated exposure to bright sunlight has an increasingly adverse effect on dark adaptation. Exposure to intense sunlight for 2 to 5 hours causes a definite decrease in visual sensitivity, which can persist for as long as 5 hours. This effect can be intensified by reflective surfaces such as sand and snow. At the same time, the rate of dark adaptation and degree of night vision capability are decreased. Since these effects are cumulative and may persist for several days, use military neutral-density sunglasses or equivalent falter lenses in bright sunlight when night operations are anticipated.

Night vision scanning. Dark adaptation or night vision is only the frost step toward maximizing the ability to see at night. Night vision scanning can enable you to overcome many of the physiological vision limitations and can reduce the visual illusions that so often confuse the observers. The technique involves scanning from right to left or left to right using a slow, regular scanning movement (Figure C-8). Although both day and night searches employ scanning movements, at night avoid looking directly at a faintly visible object when trying to confirm its presence.

Use of off-center vision. Viewing an object using central vision during daylight poses no limitation, but this technique is ineffective at night. Limited night vision is due to the night blind spot that exists during periods of low illumination. To compensate for this limitation, use off-center vision. This technique requires you to view an object by looking 10 degrees above, below, or to either side of it, rather than directly at the object. This procedure allows the peripheral vision to maintain contact with an object (Figure C-9).

Countering the bleach-out effect. Even when off-center viewing is practiced, the image of an object viewed longer than 2 or 3 seconds tends to bleach out and become one solid tone. As a result, the object is no longer visible and can produce a potentially unsafe operating condition. To overcome this limitation, be aware of the phenomenon and avoid looking at an object longer than 2 or 3 seconds. By shifting your eyes from one off-center point to another, you can continue to pickup the object in your peripheral field of vision.

Shape or silhouette. The ability to visually make out shapes is significantly reduced at night; consequently, you must identify objects by their shape or silhouette. They must become familiar with the architectural design of structures, vehicles, equip ment, and like objects, common to your AO to maximize information collection. Your success using this technique comes from extensive drill and practice.

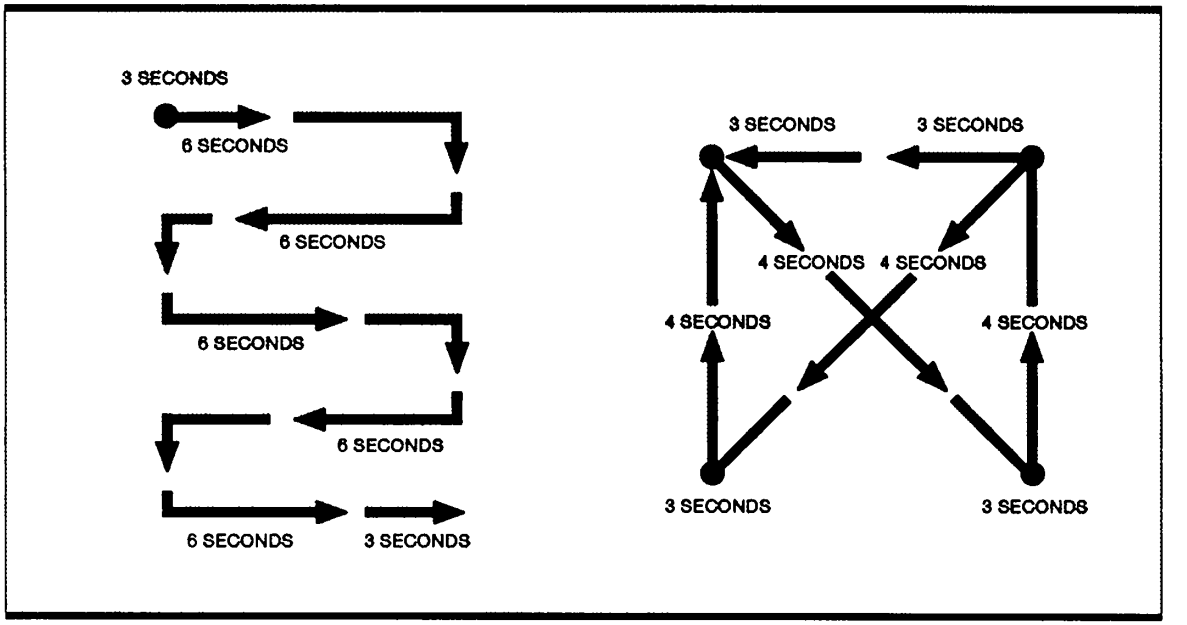


Figure C-8. Night vision scanning techniques.

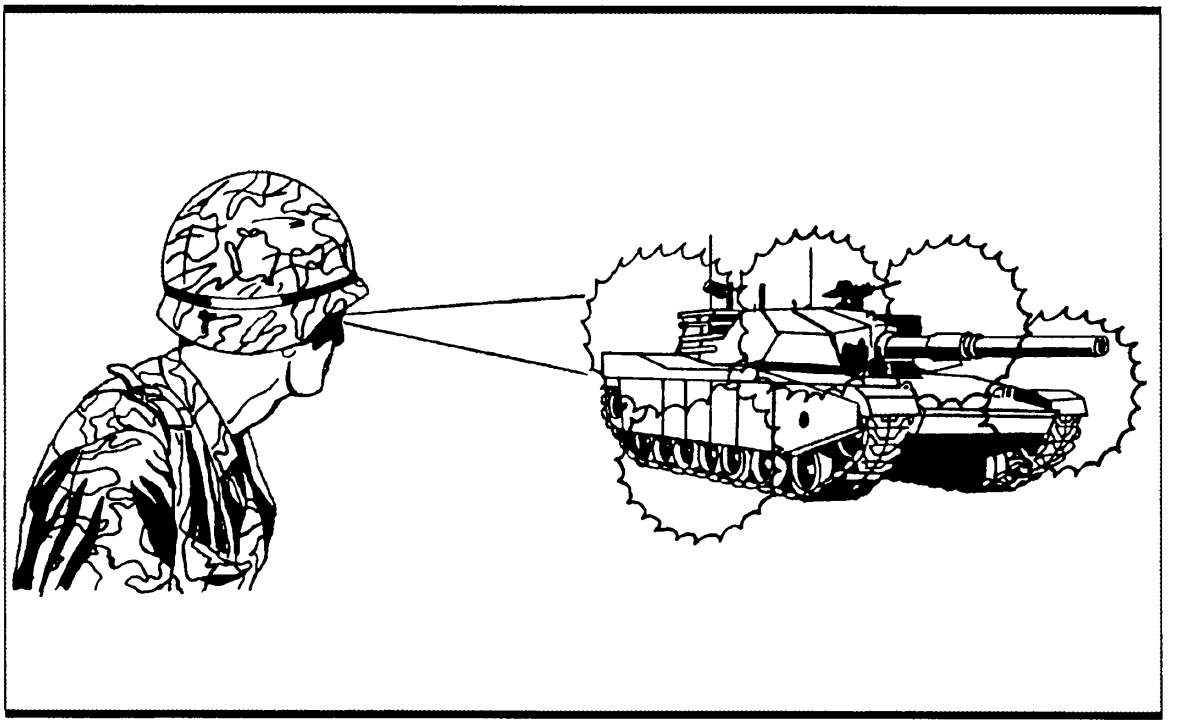


Figure C-9. Off-center vision techniques.

Light Sources and Distances. During periods of limited visibility, be cognizant of the types and ranges of different light sources. Figure C-10 lists typical light sources and the distances they are visible to the naked eye in clear, cool air.

Night Vision Devices. Because of their harmful effect on your night vision, use electronic NVDs for special applications and not for routine observation. Scan with NVDs only for a few moments using the same pattern used with the naked eye. To avoid detection, use all NVDs in the passive mode in all but the most extreme cases.

Vulnerabilities to Detection

Fixed sites are vulnerable to a wide range of compromising factors. Compromise generally results from poor site selection; faulty camouflage; poor light, noise, and smell discipline and sometimes by effective search patterns on the part of the threat force. Most compromises due to these factors occur—

- When an infiltration platform is observed.
- During movement to target area.
- When the site is being set up or occupied.
- When observers are changing shifts.
- Where the vision slit appears as a dark horizontal strip in some terrain feature.
- Where a dark spot occurs in a tree against a background of surrounding trees.
- When light reflects from the glass of optical instruments.
- When threat forces notice changes in the shape or color of terrain features and vegetation.
- When threat forces detect small groups of people appearing at approximately the same time and place (for example, for relief of observers, the serving of food, and the like).
- When a source of infrared radiation, thermal radiation, or electronic emision is detected.
- In winter, where there is an absence of frost or snow on certain tree branches.
- When there is movement of a tree in still air and nervousness on the part of birds and other animals in the area.
- In cold weather, where a wisp of smoke or steam appears from the heating of a fixed site.

Departure

When departing the site, leave quickly, quietly, and thoroughly remove all equipment, notebooks, trash, and like items. Pack ponchos and camouflage netting and, if practicable, fill in excavations. If you can fill in your excavation, carefully replace the original topsoil and original vegetation that was preserved on the site. Cover your tracks and otherwise leave the site in as close to original condition as possible. If you do not, and the site is subsequently discovered by threat forces, your presence will have been compromised. Knowing the location of the site may permit threat forces to surmise what information has been gathered. This compromise, in turn, may inhibit subsequent surveillance operations against the target. When departing the site, as a countertracking and security means, do not move directly to its ORP, patrol base, or rally point. Make frequent listening halts

en route to these locations, taking advantage of cover and concealment and making several changes in direction during movement.

CAMOUFLAGE AND CONCEALMENT TECHNIQUES

Concealment from observation is one of the main conditions for successful reconnaissance. If fixed site construction requires excavation, the principal problems are observer concealment during construction, removal of dirt, camouflage of leftover dirt, camouflage of the site during construction, and waste removal.

Concealment of Observers

In almost every case, construct an observation site at night, which affords significant concealment of your activities. The first stage of construction is the erection of a black Hessian net or other camouflage screen for you to work behind. When working on the site, do not rise above the screen. This net or screen is secured to local cover with bungee cords or 550 cord. Then emplace a poncho or other cover on which a precut camouflage net is attached, which is then erected as overhead cover. Ensure no branches are broken and no other marks are left on the local vegetation.

LIGHT SOURCES AND DISTANCES OF VISIBILITY IN CLEAR, COOL AIR

SOURCE	DISTANCE
VEHICLE HEADLIGHTS 4–8 KM	4–8 KM
MUZZLE FLASHES FROM SINGLE CANNONS	4–5 KM
MUZZLE FLASHES FROM SMALL ARMS	1.5–2 KM
BONFIRE	6–8 KM
FLASHLIGHTS (WHITE LIGHT)	1.5–2 KM
LIGHTED MATCH	UP TO 1.5 KM
LIGHTED CIGARETTE	0.5–0.8 KM

NOTE: For observation from elevated positions or the air, these distances are increased by a factor of two or three.

Figure C-10. Light visibility chart.

Removal of Dirt

Carefully outline the dimensions of your excavation and remove the topsoil and vegetation to a poncho or other material from which it may later be used to camouflage the site. Transport excess dirt from the site in anything that can be used as a container, such as sandbags and empty rucksacks. In an underground site, most of the excavated dirt is placed back on top.

Camouflage of Leftover Dirt

During construction, remove the left-over dirt so it will not attract the attention of threat forces and can easily be retrieved when the excavation is being filled in. One method of hiding the dirt is to scrape the surface underneath brush, spread the fill, and then cover it with the scrapings (being careful to present as natural an appearance as possible). Another method is to look for a natural depression, remove the top cover, fill in the depression with the dirt, and replace the top cover. During heavy rains, when runoff naturally stains surface waters, dirt can also be dumped into streams and/or other waterways.

Camouflage of the Observation Post During Construction

While constructing an observation site, maintain camouflage discipline. Work diligently to minimize exposure to the threat. Minimize disruption of the surrounding terrain. Use the dirt and topsoil that was placed on a poncho or plastic sheeting for camouflage of the site. Maintain individual camouflage to the extent possible, for example, by donning gillie suits during construction. Use natural vegetation and/or other camouflage to conceal parts of the site already completed. Continue to camouflage the site to the extent possible through its completion.

Waste Removal

For health and security reasons, maintain a high state of personal hygiene while on surveillance operations. Human waste, in particular, presents a problem. Retain the dirt from excavations to fill over in layers the human waste deposited in the excavations. Waste can be deposited in zip-leek plastic bags, MRE bags, and trash bags (that are afterward sealed). To minimize odor, use lime, baking soda, or formaldehyde. Before leaving, remove all waste or bury it so that it is not detected by personnel or dug up by animals.

DETECTION AVOIDANCE TECHNIQUES

Avoiding compromise is a prime concern of every soldier. SF soldiers have developed techniques that assist in avoiding detection. Some examples are discussed in the paragraphs below.

Stealth and Movement Techniques

Drill and practice a variety of stealth and movement techniques. Drill and practice are especially critical for reconnaissance. Basic movement techniques, including immediate action drills, are covered in TC 31-29. Stealth techniques are important for the reconnaissance of defended targets, where you may have to take up to several days to move a few hundred meters up to and around a target. Use basic stealth techniques, including any movement techniques that allow low profile, slow movement, stealth, and the use of a gillie suit. You can develop and train for many other stealth techniques on the basis of METT-T.

Tracking and Countertracking

Another set of basic SR mission skills is in tracking and countertracking. Tracking is used to acquire a moving target. Countertracking is used to avoid compromise and capture.

Tracking. Personnel, animals, and machines leave signs of their presence as they move through an area. Detection and identification of these signs may yield valuable information in and of themselves or may lead to the acquisition of even more valuable information. Visual tracking is the art of following such signs. This skill is best acquired through intense study and practice under operational conditions. The six concepts of tracking are displacing, staining, weathering, littering, camouflaging, and interpreting. See FM 21-76.

Countertracking. Countertracking techniques can minimize telltale signs that the threat force can use against you. Observation of the mistakes being made by the threat force enables the SFOD more carefully. Be conscious of the way you exit a stream, cross a trail, or move cross-country. Be security conscious at all times. Basic countertracking techniques you may employ include scent masking and direction changing.

Scent masking. Before starting an operation, follow the dietary and personal hygiene practices of the people in the area in which you are operating so that you smell as the locals do. Further masking may be accomplished by standing in smoke from a wood fire, particularly if fires are common to the AO. As an added precaution, attempt to approach the target from downwind and avoid populated areas.

Direction changing. To find out if you are being followed, circle back and observe your trail for pursuers. To shake off trackers—

- Make sudden, random changes in direction of 90 degrees or more.
- Walk several meters downstream before emerging from streams that must be crossed.
- Walk over hard bare ground, or in areas of drifting sand or snow, walk into the wind before making a radical change in direction.

Detection by Animals

In most areas of the world, dogs and other inquisitive animals can be found. A small pellet or BB gun can scare away these pests quietly; however, the weight of the gun and the space it takes up may not justify the benefits it provides.

APPENDIX

B

RECONNAISSANCE METHODS

When conducting SR operations, SFODs may employ patrols, establish observation or listening posts, emplace sensors or other special equipment, or conduct clandestine target penetration directly or through surrogates based on the IPB processes and overlays. SR is used to locate high-value military targets accurately for deep-attack weapons systems; to assess friendly, hostile, and uncommitted third-party strengths and weaknesses; and to perform other collection tasks that are beyond the capabilities of traditional military reconnaissance and surveillance units, creating windows of opportunity for decisive action. In performing their missions, SFODs employ two methods of reconnaisssance— zone and area reconnaissance.

ZONE RECONNAISSANCE

Zone reconnaissance includes operations conducted to obtain information on the threat, terrain, and routes within an area. The principal purpose of using SFODs against such targets as industrial facilities or LOC is to monitor their status and activities for use in a follow-on or standoff attack. SR targets are normally located beyond the capabilities of conventional reconnaissance means. Zone reconnaissance teams reconnoiter one specific objective and its immediate surrounding area using long- and short-range surveillance and/or vantage points. An SFOD may conduct one or more area reconnaissances within its zone based on its mission analysis. Zone reconnaissance missions may require more than a single SFOD. When two or more SFODs are used in a zone, close coordination is required. Mission planners should consider splitting the zone into smaller sections. If such a split is not feasible, the planners should clearly define boundaries. Zone reconnaissance includes use of the fan, converge, successive-sector, and "L," "U," "W," and "Z" techniques.

Fan

In the fan technique, SFODs leave an objective rally point (ORP) and return to the same ORP. As shown in Figure B-1, page B-2, SFODs move out of and enter the ORP at opposite sides and move in the same clockwise direction to eliminate the chances of accidental contact between the elements. They may survey their routes singularly or simultaneously. The routes must be planned so that SFODs do not converge and interfere with one another. This method tends to compromise the location of the ORP after a time because of frequent movement into and out of the ORP. Therefore, SFODs should relocate the ORP often. They must ensure enemy trackers don't follow them back to the ORP.

Converge

In the converge technique, SFODs move through areas on converging routes. Beginning at an ORP where elements are briefed, they move on separate routes through the area and converge at the end of the area at a rendezvous point. The SFOD leader briefs each element on the route it is to take, the location of the rendezvous point, and the linkup time at the rendezvous point. As shown in Figure B-2, the SFODs start their sector reconnaissance in the same relative direction from their rally points (RPs) and move in the same counterclockwise direction to prevent chance contact.

Successive Sector

In the successive sector technique, SFODs may divide the objective area into segments and assign each element a segment. As each element moves at its own pace until it completes its part of the reconnaissance, no time is wasted in waiting. It also allows element leaders more freedom of action. The SFOD leader may only dictate the general direction of movement the elements will take in their AO, the time for completion, and the linkup or rally point. Figure B-3 shows the use of two techniques and an optional third that may be used by reconnaissance elements.

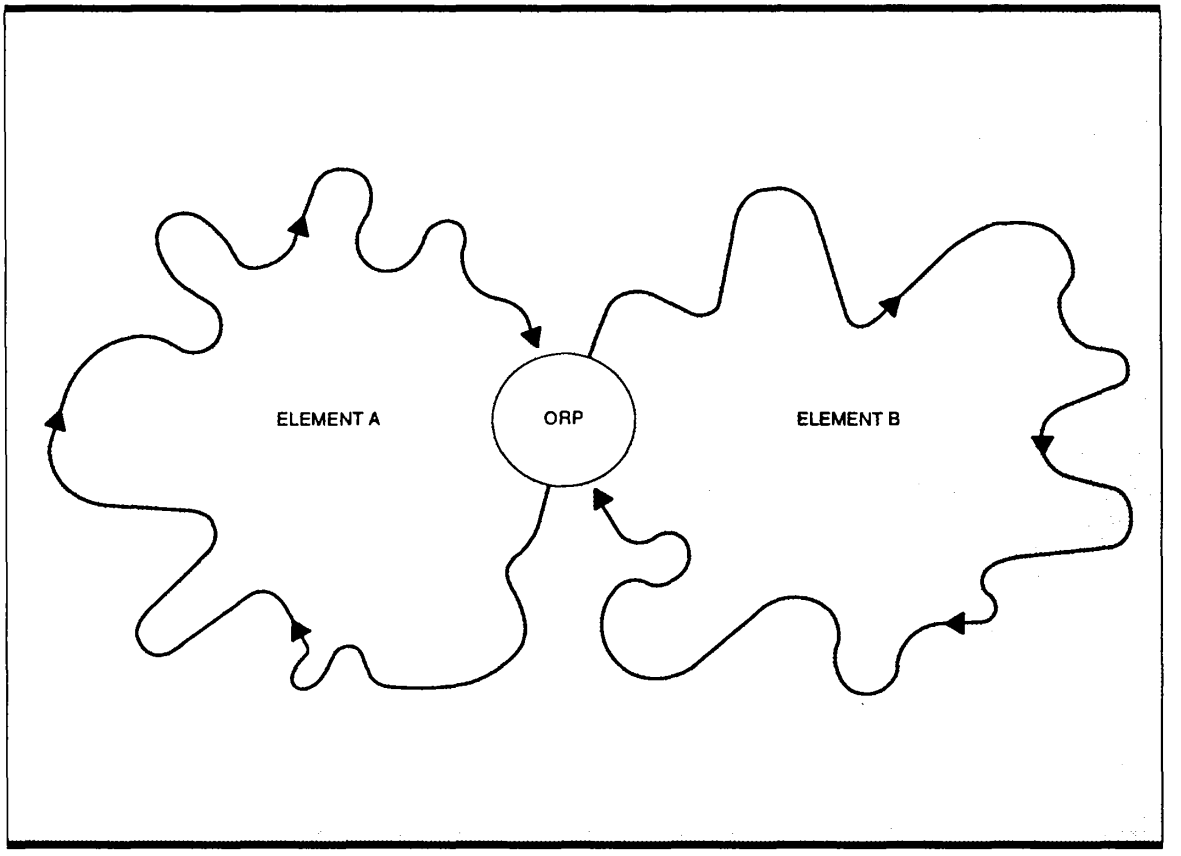


Figure B-1. Fan technique.

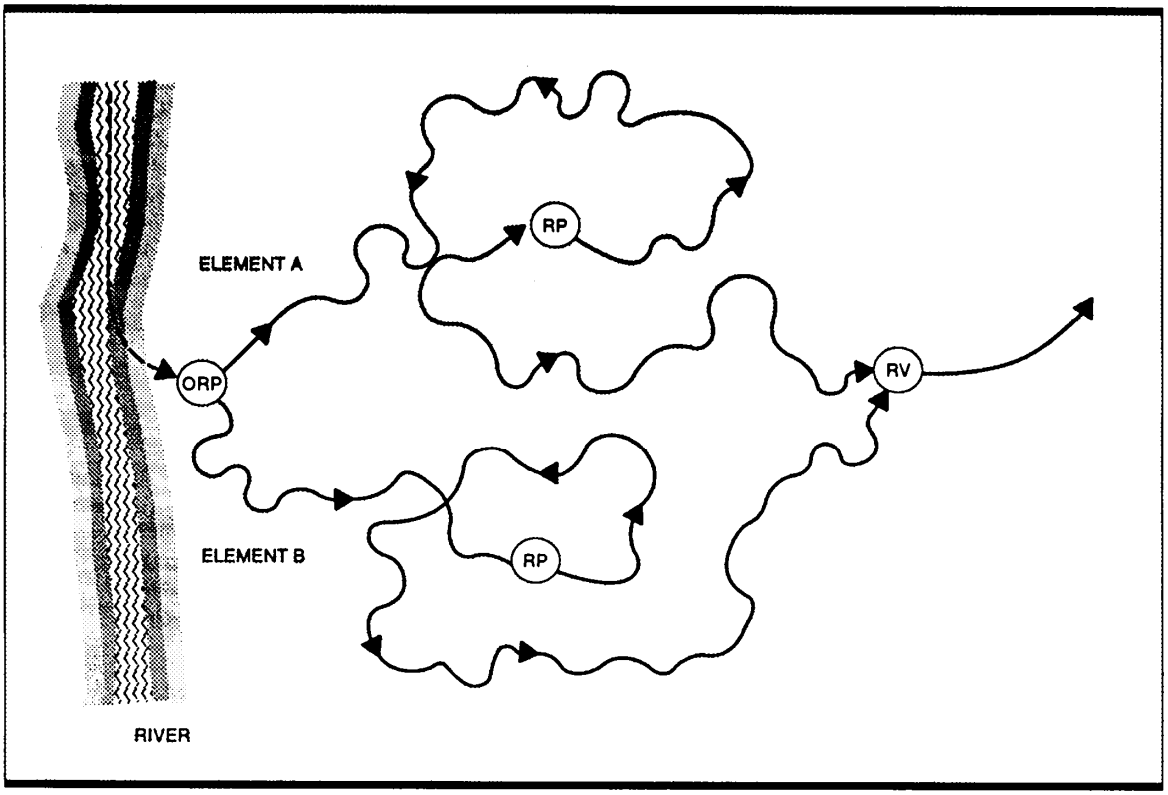


Figure B-2. Converge technique.

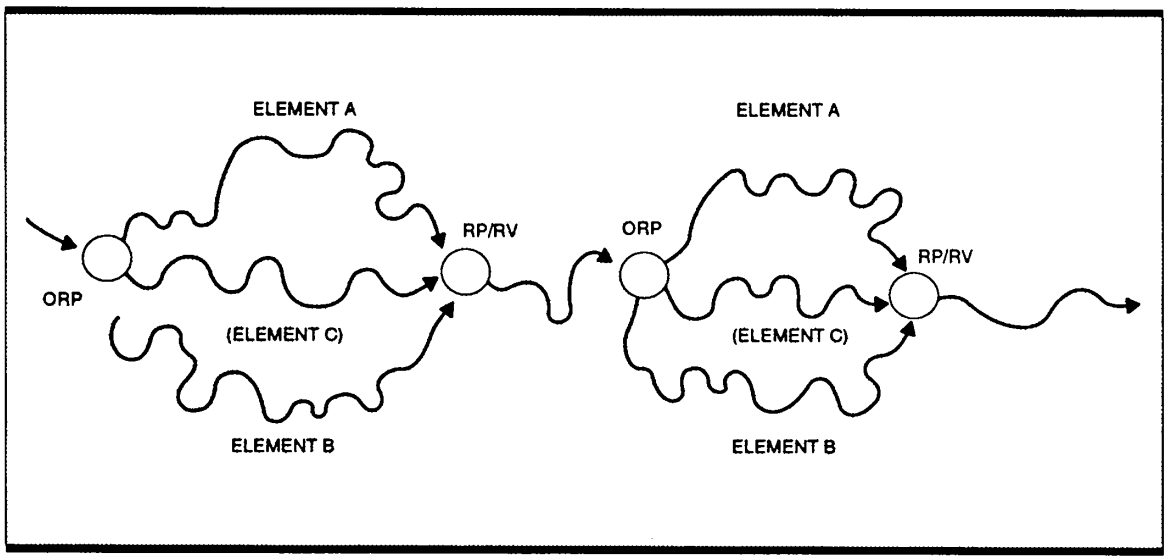


Figure B-3. Successive sector technique.

"L" "U," "W," and "Z" Techniques

It is generally impossible to completely survey over-sized patrol sectors. In such situations, the SFOD must therefore plan to employ a technique of cross-country movement that will provide the best coverage consistent with the mission, threat force disposition, weather, and terrain. It is important that the SFOD move in a way that will permit it to intersect LOC, linear obstacles, and that forces, especially in an area about which little is known of the threat and/or terrain. Basic movement techniques used for surveying specific patrol sectors in such situations include the "L", "U"," W", and "Z" techniques as illustrated in Figure B-4. In all cases, the patrol inserts at one point in its sector and is picked up at another distant point. In most cases, threat forces, weather, and terrain preclude following a model pattern, but the principle remains valid.

Route or Corridor Reconnaissance

A variation of zone reconnaissance is route or corridor reconnaissance. Route or corridor reconnaissance obtains information on the targeted activity, obstacles, route conditions, and key terrain features (Figure B-5). Reconnaissance and classification of existing vehicular routes can be of great importance in determining the mission capabilities of the target complex and taking appropriate follow-on actions. SFODs normally generate ROUTEREPs and BRIDGEREPs in route or corridor reconnaissance. See Appendix D. For more information on route reconnaissance, refer to STP 31-18C34-SM-TG.

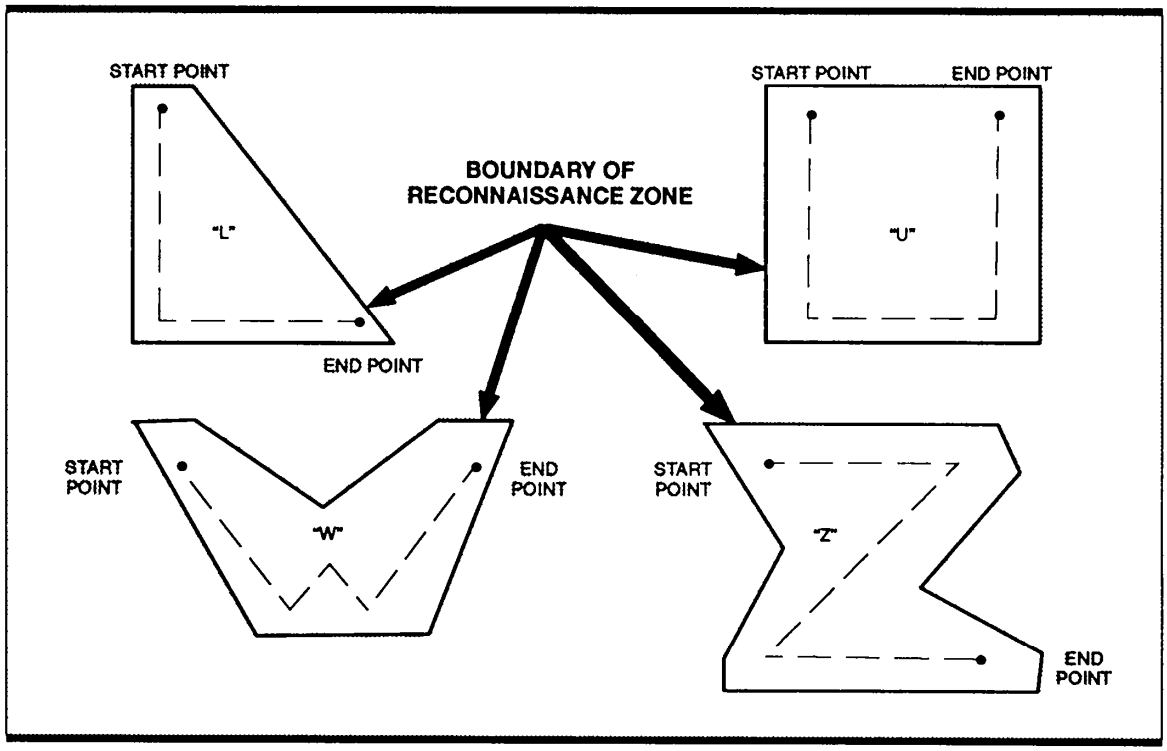


Figure B-4. "L," "U," "W," and "Z" techniques.

AREA RECONNAISSANCE

An area reconnaissance is a survey of a specific location such as LOC choke, special weapons storage sites, launch sites for such weapons, industrial plants, or terrorist safe houses (see Figure B-6, page B-6). The basic purpose of using SFODs in this context is to provide real-time and NRT information on status, disposition, and significant activity to predict threat activities and/or generate enough information for a friendly reaction.

As in Figure B-7, page B-6, area observation is accomplished by maintaining OP surveillance on the target, usually a known or suspected choke point, position or activity. When SOT A augmentation is available, there may also be an additional SIGINT OP surveying the target.

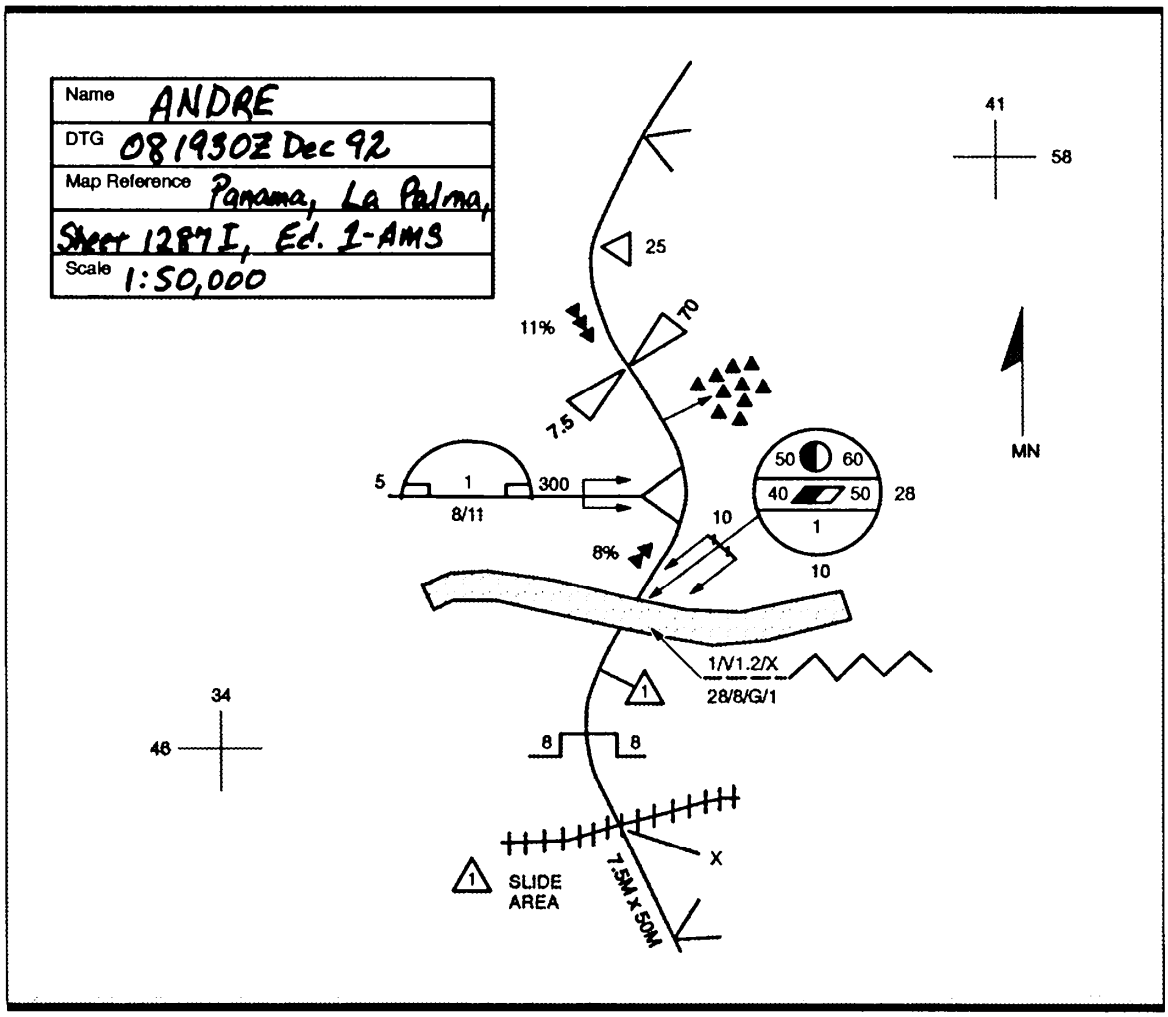


Figure B-5. Route and/or corridor reconnaissance.

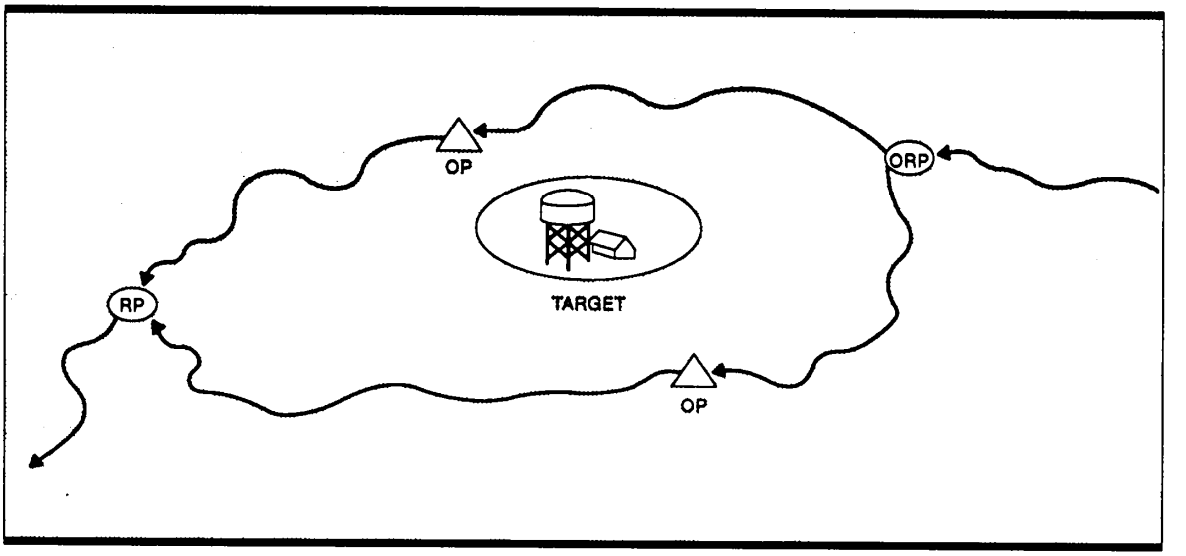


Figure B-6. Observation of a specific point.

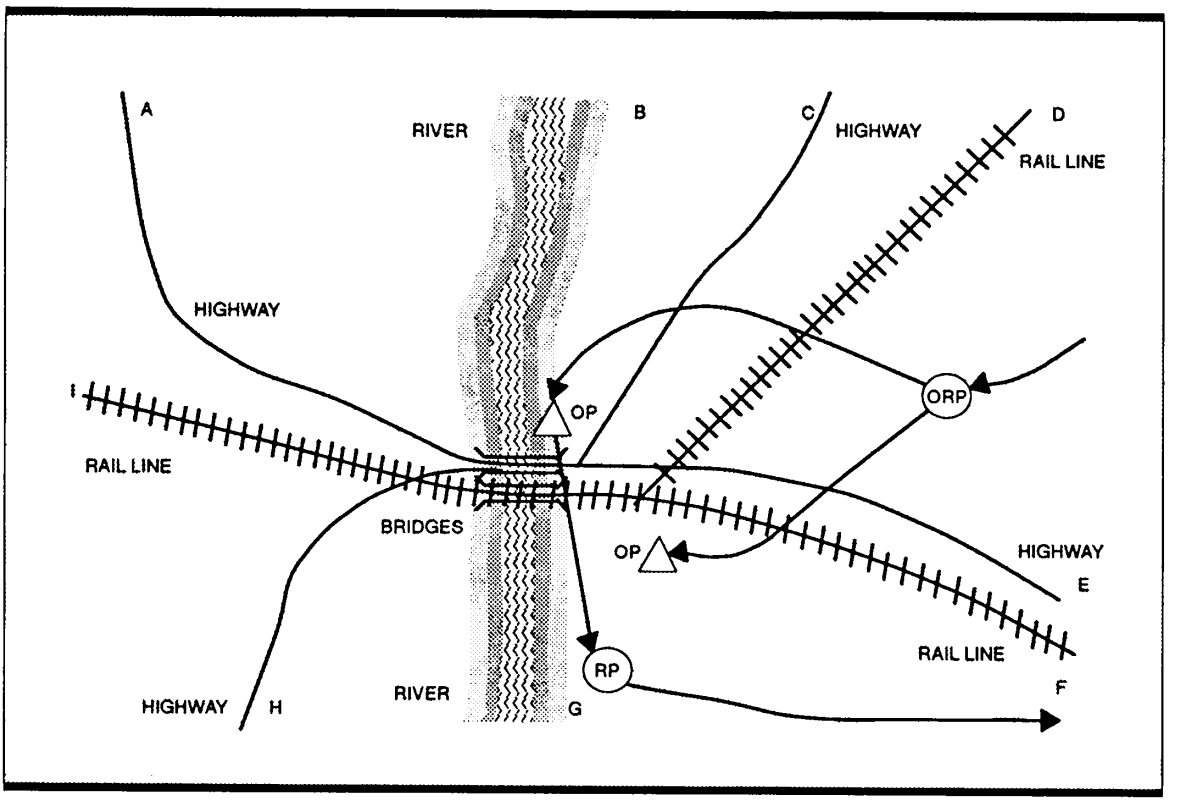
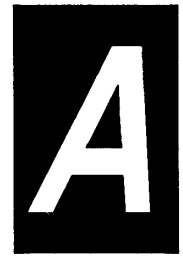


Figure B-7. Choke point observation.

APPENDIX



FIXED OBSERVATION AND SURVEILLANCE SITES

An observation and surveillance site can be a prone soldier in a defensive position. The site might also be an elaborate underground complex constructed with polyvinyl chloride (PVC) pipe and canvas with connecting transmisson sites. The type, location, and operation of the site depend mainly on METT-T factors. If during mission planning, the SFOD determines that fixed site is required, then site selection, security, construction, and occupation must be planned in detail, and practiced. The variables associated with fixed SR sites are the geographic regions in which the operation will take place. This appendix addresses the process of selection, construction, and occupation of fixed observation and surveillance sites used in permissive and nonpermissive areas around the world. During this process, the SFOD should apply the acronym "BLUES" (Figure A-1).

URBAN SURVEILLANCE SITE

An urban or built-up area forms the economic and cultural focus for the surrounding area. It is characterized by a concentration of man-made structures, facilities, and a population. SFODs may conduct fixed and mobile surveillance in urban areas. Because of the generally limited fields of vision, urban operations normally require more sites than rural operations. See FM 90-10.

B lend in with the surrounding area. Does the site look natural? Does it attract unwanted attention?

L ow to the ground construction techniques must be used. Does the site provide protection against small arms and direct weapons fire?

U nexpected sites should be used. Will the threat forces expect you to look out the window or the small hole in the wall?

E vacuation routes must be planned during site selection. Where will you go to link up with the remaining SFOD members if you are discovered or overrun?

S ilhouetting the site is avoided by using the sides not the crests of hills. Can the sniper see you silhouetted against the skyline, wall, or other object?

Figure A-1. "BLUES" application.

Site Selection

METT-T dictate urban site selection as with other observation and surveillance sites. SFODs can construct fixed urban sites in occupied and abandoned buildings, water tanks, shrubbery, on factory chimneys, or in the attics of multistory buildings or other tall structures. If possible, SFODs should avoid wooden buildings and buildings in a significantly deteriorated condition because of the risk of injury from fire and/or structural failure.

Permissive and Semipermissive Environments. If operating in urban areas in a permissive or semipermissive environment, surveillance teams may be mobile, using indigenous transport such as taxicabs, military vehicles, trams, bicycles, and subways. Taxicabs often have the advantage of having two-way radios. In such environments, fixed and overt sites may be emplaced to serve as a deterrent by virtue of their mere presence. Where sites are overt, they must be mutually supporting and hardened enough to withstand threat attacks.

Nonpermissive Environments. If operating in a nonpermissive environment, fixed sites should not be in buildings that attract the threat's attention but should be in rubble, yards, and gardens. If the site is to be set up in an undamaged part of the urban area, the SFOD should select buildings of solid construction with serviceable stairs and basements that can be equipped for the rest and shelter of personnel during artillery bombardment.

Construction

Site construction may consist simply of taking a position by a suitable viewing port, or it can be much more elaborate. If the SFOD plans to use the site for an extended time, it must take steps to improve site survivability and its ability to fight fires. Windows, doors, and other openings (like bullet holes not used for observation) are filled with bricks, fragments of building materials, or sand bags if available. Flammable objects are removed from the premises. The SFOD performs all construction while keeping in mind operational security. Supplies of water and sand are assembled for fighting fires. If the threat has previously occupied the building, the SFOD takes precautions against booby traps and mines. Where the threat is near, several places in the building are prepared for observation and departure. Interbuilding monitoring and SFOD communications are hard wired if wire is available although fiber optic cables, if available, offer better security.

Vulnerabilities to Detection

The higher concentration of people, security forces, lighting, and movement in urban areas require SFOD members to take additional precautions to avoid detection during their surveillance activities. SFODs in such situations may comprise teams of as few as two people, working in civilian attire and employing safe houses. Intra-team communications may require very low-power radios and the use of specialized technical and nontechnical communications means as a last resort when other means are inadequate or impractical. If operating from an occupied dwelling in a denied or contested area, the SFOD must be careful not to consume more electric power or water than usual or more heating fuel or focal

than average for the normal occupants. Security forces have been alerted to the presence of SFODs by such minor indicators as sudden increases in milk deliveries. Electronic countermeasures (ECM) technology has also advanced to a point where mobile units operating from the street can electronically survey a building and detect and identify very small sources of energy. This type of ECM intensifies if the presence of an SFOD is suspected. Such capabilities are increasingly widespread and are often found in built-up areas of even marginally developed countries, especially in the "security states" of the Third World. As a result, urban operations require extremely detailed planning in electronic counter-countermeasures (ECCM).

MOUNTAINS

Mountainous areas are characterized by rugged, poorly trafficable terrain, steep slopes, and elevations above surrounding areas. The number of observers and sites required may be increased in mountainous terrain due to the relatively limited fields of vision compared to flat terrain. However, in areas above the tree line, or when lower elevations lack vegetation, the number of observers may be decreased. A careful study of the target area will give a good indication of the requirements. For a general discussion of operations in mountainous areas, see FM 90-6.

Site Selection

Mountain terrain provides many places for cover and concealment. Site selection is not guided by the height of a given mountain but by the irregular fields of observation, dead spaces, cover and concealment, and the limits of the observation equipment used by the SFOD. The SFOD may employ a circular, multitiered system of observers. To increase the daytime viewing capability, the SFOD situates sites not only laterally but also with vertical dispersion. This layering of sites also reduces the need for movement when changing from daytime to nighttime operations. Since movement is the main cause of compromise, layering sites also adds to the security effort of the deployed SFOD. (See Figure A-2).

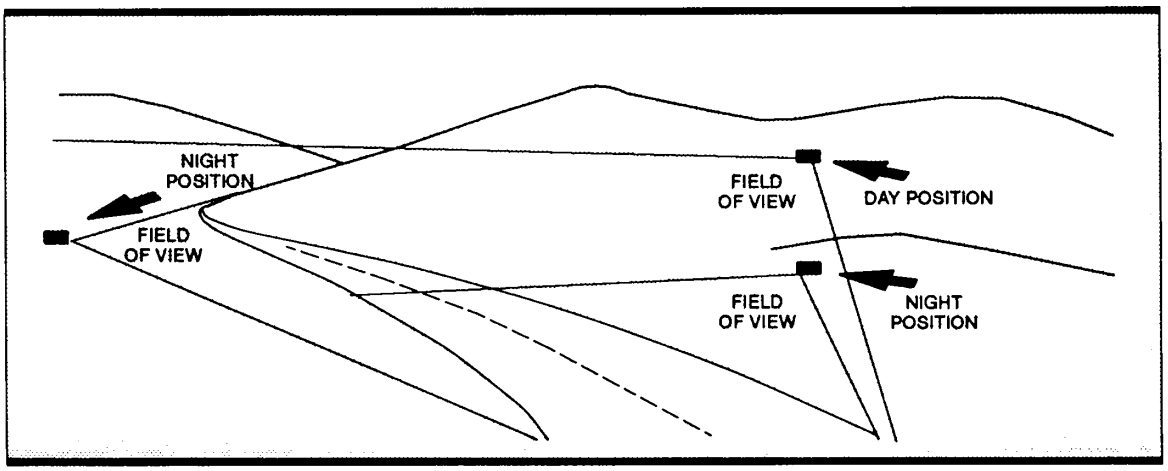


Figure A-2. Overlapping mountain observation sites.

Construction

Irregular terrain in mountains often affords natural hiding places for observers. In most mountainous areas, the rocky nature of the ground makes it difficult and often impossible to dig below-ground sites. In those cases, the SFOD may use boulders and loose rocks in above-ground construction of low-walled sites called "scrapes." When these sites are constructed, SFOD members use the same degree of care in camouflage as they use in the case of all other types of construction. The site must blend in with its surroundings and not be detectable from any angle. Fields of view can often be enhanced if the lower branches on the undergrowth are trimmed back with a wire saw, shears, or knife.

Night Observation

At night, the SFOD may enhance observation in mountainous areas by sending out additional observers into valleys and hollows. Observation from below upward against the background of the sky often gives better results. Moreover, the SFOD should supplement night observation by monitoring. Monitoring is more effective in mountainous areas than on flat terrain, since sounds are often funneled to the head of valleys and are perceptible at great distances. However, sounds in the mountains can be deceptive. Various obstructions can reduce their volume and change their direction.

Snow

In mountainous areas, where snow is expected or known to be on the ground, SFODs can use certain tactics to reduce the problems associated with operations in the snow. Some of those tactics are discussed in the following paragraphs.

Fixed Site Selection. While conducting a map reconnaissance of the AO in isolation, the SFOD chooses sites that are in shaded areas, on slopes facing away from the equator (north in the Northern Hemisphere, south in the Southern Hemisphere). This preliminary site works to the advantage of the SR mission as described below.

In moderate temperatures, the heat generated from the observer's bodies melts the snow on the cover of the site. The result is an unexplainable muddy area in snow. Such melting is, however, common around trees. The melting snow during the heat of the day often falls to the ground and, in turn, melts the snow on the ground. The melting snow falling off the trees often can be used as a water source. Unlike snow, this water source does not require melting over a heat source. The shadows found around rock outcropping and trees also aid in hiding the foot trails leading to the work area and site. The shade aids in an even melt. Even melting helps prevent compromise. Walking compresses snow under each footprint. The compressed snow melts at a slower rate than the surrounding snow. This effect is like comparing the difference between crushed ice and cubed ice in a drink. The loose, crushed ice melts faster than the dense cubes. In areas where the snow melts fast, such as a sunny side of a hill, the compressed snow will leave footprints or trails leading to the site.

The constant daytime melting and nighttime refreezing of snow on slopes often results in avalanches. Reducing the risk of avalanches can be done by using shadows and shaded slopes. Most danger areas are well known and are often plotted on military and civilian maps.

Mission planners consider the advantages and disadvantages of using the infiltration aircraft very close to the target area. In remote areas of hard packed snow, the rotor wash left from a low-hovering helicopter may be more desirable than long trails that can be easily tracked.

Information on Snow Conditions. Multiple sources are often available for obtaining information about the snow conditions in different areas of the world. One of the most often overlooked is area tourist information services. In many countries, these services are often free and available to everyone. Also, information on areas susceptible to avalanches is often available through maps, national or state forest services, or other government services. The SFOD may also get information on daily snow conditions from area ski resorts. Combining this information with that obtained from the regular weather services can provide the mission planners with a detailed picture of the area.

DESERT

Deserts have a low-average rainfall and a lot of sunshine. Plants and discernible terrain features are scarce in these regions. Deserts are characterized by sand storms, dust, fog, and haze. The temperature may change 100 degrees Fahrenheit (48 degrees Centigrade) between the hot days and the cold nights. These are but a few of the problems that an SFOD will face when employed in the desert.

Navigation

Determining the exact position of an SFOD or target on the ground is very difficult. Only distant terrain features, mirages, and the changing climatic situation hinder navigation. Recently, however, global positioning systems have been developed to locate positions through the use of satellites. All units employed in desert regions should obtain one or more of these invaluable tools.

Observation Techniques

Mirages will affect observation in desert country. Frequently checking the terrain against the map aids the observer. However, training and experience play a critical part in accurately reporting the activities of the target. The SFOD pays special attention in the still, early-morning hours when targets are not concealed by clouds of dust close to the ground. During the day, however, the wind may disrupt or destroy camouflage completed during the night and make identification of threat positions considerably easier. Routine “stand to” actions during sunrise may provide the best information of the day.

Optical Aids

Optical aids play a big part in mission success in desert regions. These aids may range from binoculars to high-powered night vision telescopes. Standard binoculars prove effective, even during the hours of darkness. Optical aids must hold a special place in the unit’s METL and be used routinely during training.

Desert Vehicles

Vehicles are normally used for desert observation and surveillances due to the vast distances covered. However, fixed sites may be used as well. Where fixed

sites are used, the positions are normally buried or semiburied because of the lack of cover and concealment. Often these positions are as much as 15 degrees Fahrenheit (8 degrees Centigrade) coder than the surrounding terrain and permit the SFOD to operate for a longer time in the area.

Site Construction

Deserts often have rocky soil or "surface chalk" soil, which makes digging difficult. Disturbing this "chalk" is a major concern when digging subsurface sites. In most desert areas, rocks and boulders are often used in site construction. Underground sites are also difficult to construct in soft, sandy areas because of sidewall instability during construction, occupation, and use. Sidewall reinforcement is almost always required. Sandbags, plastic sheeting, and sand filled boxes may also be used for containing backsliding soil. For a general discussion of operations on desert terrain, see FM 90-3.

FOREST

Forested terrain is characterized by dense foliage, shrubs, and other vegetation, with limited fields of observation and fire. Because of the limited fields of vision, observation site selection is very important. During site selection, the SFOD considers all the options available. Surface or subsurface sites or observers in trees all have different advantages. A careful analysis of the terrain is important to the success of the mission. Old-growth and new-growth forests have different characteristics. The main difference is the height of the limbs and undergrowth. Such information is required for both site selection and planning movement times.

Ground Observation Sites

Sites on the ground are camouflaged to resemble stumps, fallen trees, bushes, and like features. For increased surveillance, the SFOD locates the site to overwatch the intersection of fire lanes, roads, and footpaths on the edge of sparsely wooded areas and natural clearings. When available, obstacles such as creeks, ditches, or steep slopes should be between the site and the probable route of security forces. At night, even a small creek causes a threat force to make noise, disrupt formations, and generally slows its progress. All of these actions are to the advantage of the SFOD.

Observation Sites In Trees

A variety of skills are required for observation from sites in trees. The equipment requirements and planning considerations are different from those of ground sites. Observers for tree sites choose trees that are situated well within the forest. They should never stand out in height, shape, or color. Observers are well camouflaged in the crown of a tree. The primary disadvantage is getting into and out of the site. Special skills and equipment are required for operations in trees. Further, the observer in the tree must be covered by fire that permits him to exit his location if detected or engaged by hostile forces. On the other hand, trees provide an advantage of a long-range view in open areas. In heavy-growth areas, the view may be nothing more than the tops of trees. This consideration can be addressed through area studies and debriefing assets during mission planning. Another advantage of tree observation sites is that most people don't look more than 2 to 3 feet above their heads when walking. When a traveler is carrying a load on

his back, he often bends forward at the waist. Both of these actions prevent him from doing little more than looking at the ground at his feet to maintain his footing. With one key exception, trees will provide good concealment for the observer even if the threat force is trying to look in the trees for him. The one key exception is when the observer is moving about in the site. Slight movements in trees can be seen and heard for vast distances. Employed SFODs consider providing the observer with a small piece of flat wood to stand or sit on. In a forest, an observer often sees less than he hears, especially at night. Monitoring the target area is critical to accomplishing the mission and providing the SFOD with operational security. The observer can monitor the target in several ways. He can sit quietly listening to sounds with his eyes closed, or he can record the sounds of the area on a tape recorder and play the sounds back at a louder volume into headphones. Remote sensors often play a key role in monitoring the target. Each SF group has sensors assigned to its MI detachment. These sensors normally are easy to use and provide outstanding results.

JUNGLE AND SWAMP

SFODs often conduct SR operations in humid, tropical areas with dense growths of trees and vegetation that reduce visibility to less than 30 meters. This thick growth provides the SFOD excellent concealment; however, movement through dense jungle terrain is impeded by a time multiplication factor of 2 or 3. For a general discussion of operations on jungle terrain, see FM 90-5.

Observation Site Construction

Most jungle sites used by SFODs are unimproved. The observers may do little more than lay on a poncho to keep dry and minimize disruption of their site. More developed jungle sites are quickly constructed using easily procurable items such as ponchos or natural materials. Planning considerations, such as high water tables, dense undergrowth, and tree roots often require above-ground construction. SFODs give primary consideration to drainage, waterproofing, and the avoidance of poisonous insects and reptiles. This technique not only prevents flooded positions but, in areas of standing water, will provide the observer the ability to listen and watch for movements in the target area.

Hammocks. Lightweight, compact nylon hammocks are invaluable in jungle regions. The hammocks can be used for sleeping or for storage of equipment. The primary advantage is that the soldier or equipment is elevated off the ground. Unlike the "swamp bed" the hammock does not require a lot of work to erect and is temporary in nature. For more information on swamp beds, read FM 21-76.

Floating Platform. The floating observation platform is a structure used in areas where ground water is high or where there is a low-pressure resistance soil. This platform provides a floating base or floor where wet or low-pressure resistance soil precludes standing or sitting. The platform is constructed of small branches or timber layered over cross-posts, thus distributing the floor load over a wider area (see FM 5-103).

NORTHERN AREAS

Observation in northern areas requires a number of special considerations. Observers must contend with extended light in summer and extended darkness in winter, along with the cold, snow, ice, fog, rain, and sleet. In most cases, operations

require at least six men to ensure continuous observation and security. Shelter is critical for protection of the men and their equipment from the elements. When using northern sites, observers must take advantage of wind breaks, such as densely wooded areas, downwind sides of terrain elevations, and depressions. Where these features are not present or their use is infeasible, observers use other expedients, such as snow caves. In general, the four basic construction materials available in cold region terrain are snow, ice, frozen soil, and timber. For a general discussion of operations on northern terrain, see FM 31-71. For a discussion of shelter construction in northern areas, see FMs 21-76 and 5-103.

PLANNING

Surveillance planning is a vital part of the SR mission. Based on the analysis of the mission and target(s) during isolation, the SFOD intelligence NCO develops a tentative reconnaissance and surveillance plan for placing the target under observation. The plan addresses the location of observation sites, the duration of surveillance, the number of personnel to be employed, and the items of special equipment to be used. Planners consider the use of sensors to expand the sector of surveillance, provide security to observers, and cover dead space. When covering a point target, 360-degree coverage is ideal but not necessary if the critical node can be observed from one site. All-around coverage may require the use of multiple sites, which, in turn, may require the SFOD to be augmented with additional personnel. However, when more personnel are involved in surveillance, the chance of mission compromise is greater. Once surveillance is established, it should be continuous; however, continuous surveillance may not always be feasible.

CONFIRMATION OF THE SITUATION

Upon arriving at the target area, the SFOD must conduct a preliminary reconnaissance to confirm the situation. The goal is to confirm the targets' exact location, ensure the maps used during planning were correct, and be the basis for selecting the actual locations of the observation and surveillance sites. Other items of interest addressed at this time include indications of threat security patrols, population control measures, LZ and DZ locations, and the best routes for movement in the area. Major changes to the situation may require revamping of the plan. If major changes to the coordinated plan are required, the new information must be passed to all supporting agencies through the SFOD's higher headquarters.

SURVEILLANCE SITE SELECTION

Surveillance sites are used for observation and monitoring. They are a vantage point from which visual, audible, olfactory, and electronic data on a target is collected. Selection of the sites is based on METT-T factors, but several general planning considerations apply. The sites—

- Afford adequate visual and electronic line-of-sight target observation and security for the observers.
- Have as wide a field of view and as little dead space as possible.

- Are not near natural lines of drift or in terrain that would naturally draw the attention of threat forces, such as atop a flat rock face on a hill.
- Have covered and concealed exit and entry points.
- Are far enough downwind from the target and inhabited areas to minimize the olfactory detection of the site by dogs or people. Keep in mind that wind directions often change at various times of the day.
- In general, are as close or distant to the target as mission and security considerations dictate.
- Have good overhead and side cover and concealment.
- Are capable of enacting battle drills to break threat contact.
- Afford reliable communications between the observers and their main body, security element, and/or communications element.
- Are, above all, in a location that is not obvious to threat forces.

If all these features cannot be found in a single site (for example, daytime versus nighttime requirements), separate sites suited to the type of surveillance performed may be necessary. Multiple sites are mutually supporting if one site is compromised, members of the other site are able to continue the surveillance mission and/or warn the rest of the SFOD. Further, if the sites are not being used during the day, they should be kept under observation. If the sites can't be secured by observation, they should not be reused the following night. This practice prevents the SFOD from walking into an ambush while trying to reoccupy the position. The SFOD avoids establishing patterns and trails while moving to and from the different sites. In all cases, the SFOD selects alternate locations for its sites if the primary sites selected on the basis of map reconnaissance prove unsuitable.

SURVEILLANCE SITE CONSTRUCTION

Surveillance sites can be surface, underground, or elevated. The SFOD designs these sites for a specific purpose, mission, or target. The primary rule for building the site is that construction must be done during darkness and the site must be occupied before sunrise. Based on METT-T, occupation before sunrise may not be practical. An overt site in a permissive environment could very well be built in daylight, or a complex site may require more than one night to build. Other planning factors such as illumination and current weather conditions also play a major role in construction and occupation of a fixed site. When all factors are considered and the final location of the site is selected, then the priority of work is the external features of the site. After occupation of the site, the SFOD can improve internal features. While planning the construction of the site, the SFOD keeps in mind that everything used for the site must be removed or replaced so that the terrain is returned to its natural state. The SFOD keeps threat forces from gaining information about the extent of the operation, possible target location, and even the fact that it was in the area. Not enough can be said of the importance of site construction rehearsals under similar conditions to the target's. When possible, the same type soil, construction materials, and planned techniques are used. During rehearsals, fellow unit members try to compromise the SFOD that has occupied the site. Weaknesses in construction or occupation plans will quickly become apparent.

Types of Observation or Surveillance Sites

When fixed sites are required for mission execution, METT-T factors determine the extent of the construction. In all cases, camouflage and concealment, as well as light and noise discipline, are important considerations during the construction of observation or surveillance sites. The following paragraphs describe different types of site construction commonly used.

Above Ground Sites. Above ground sites are the most common type of fixed observation and surveillance sites. The advantages of selecting an above ground site are the ease and speed of which the site can be selected and occupied and the simplicity of construction. The primary disadvantages in these type sites are easy detection and little protection from small arms fire compared to below ground sites.

Spider hole. This type of site is similar to a fighting position with overhead cover. The dimensions are normally about 0.75 meters wide by 1.2 meters long and 1 to 1.5 meters deep. The observer can adjust the dimensions to meet his needs. This one-man site is normally established on a line or ring to provide support and enhance security (see Figure A-3).

Scrape. A scrape is the enlargement of a depression in the ground to allow for one man to take up a position. Scrapes are hasty in nature and require little preparation. Often used during darkness, scrapes provide the observer with a position where he can better use his optical devices. The observer removes as much of the signs of occupation as possible when he leaves. He obscures the area by brushing matted grasses, displaced dirt, and footprints. overhead cover such as a poncho provides limited protection from the elements. (See Figures A-4 and A-5.)

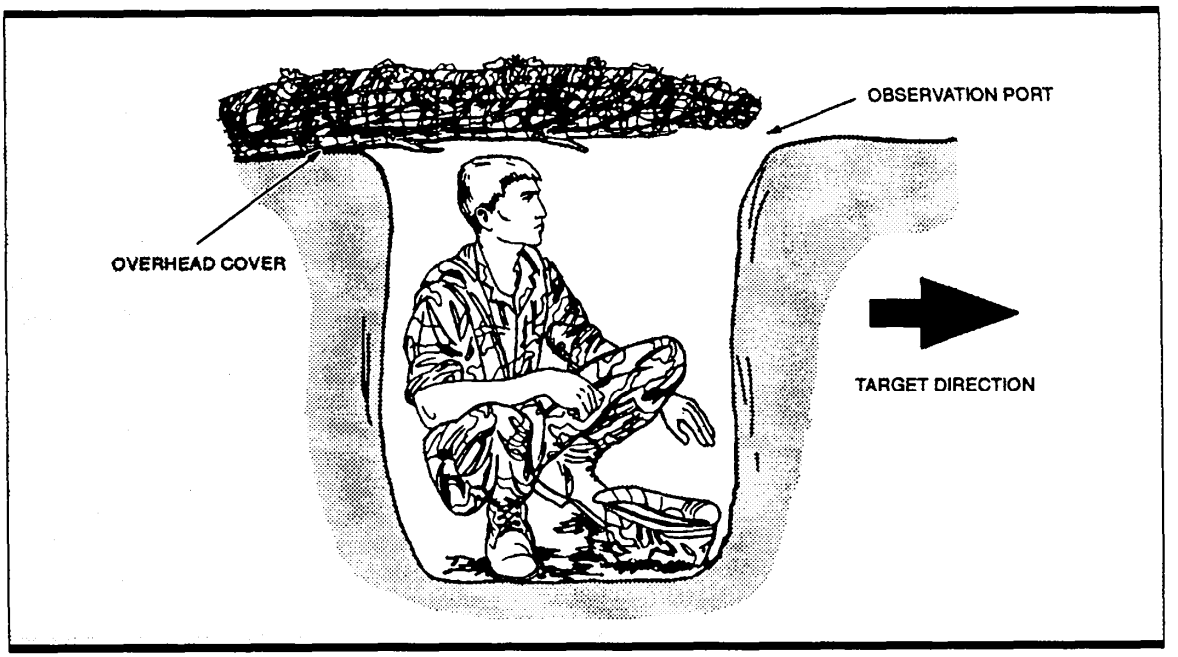


Figure A-3. Spider hole observation site.

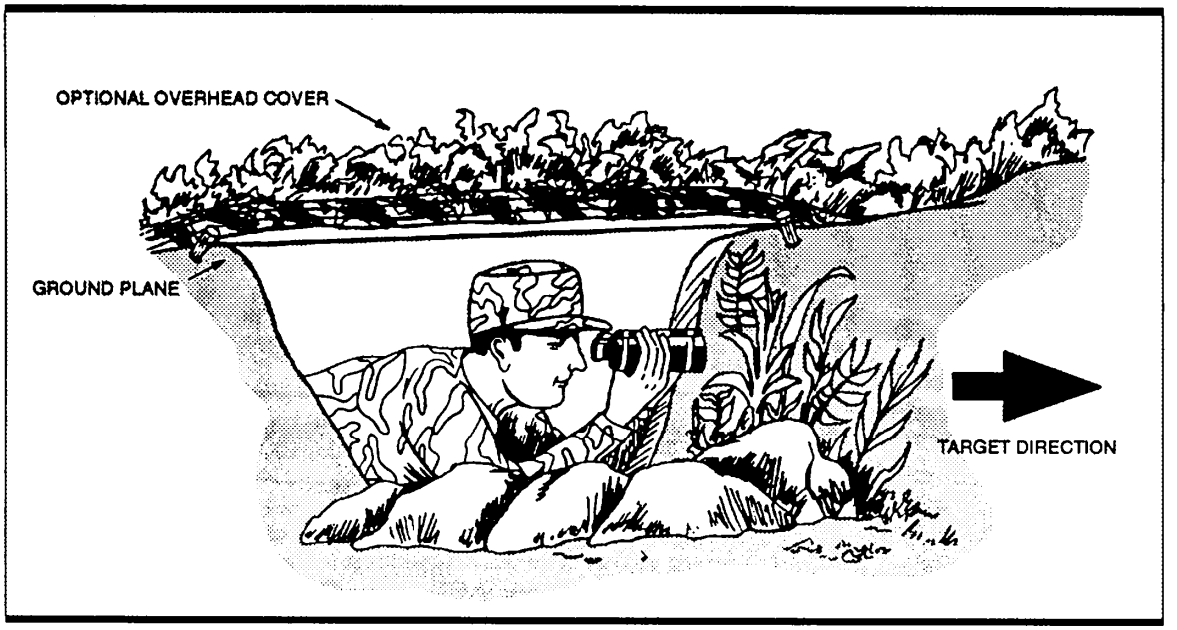


Figure A-4. Scrape-type observation site.

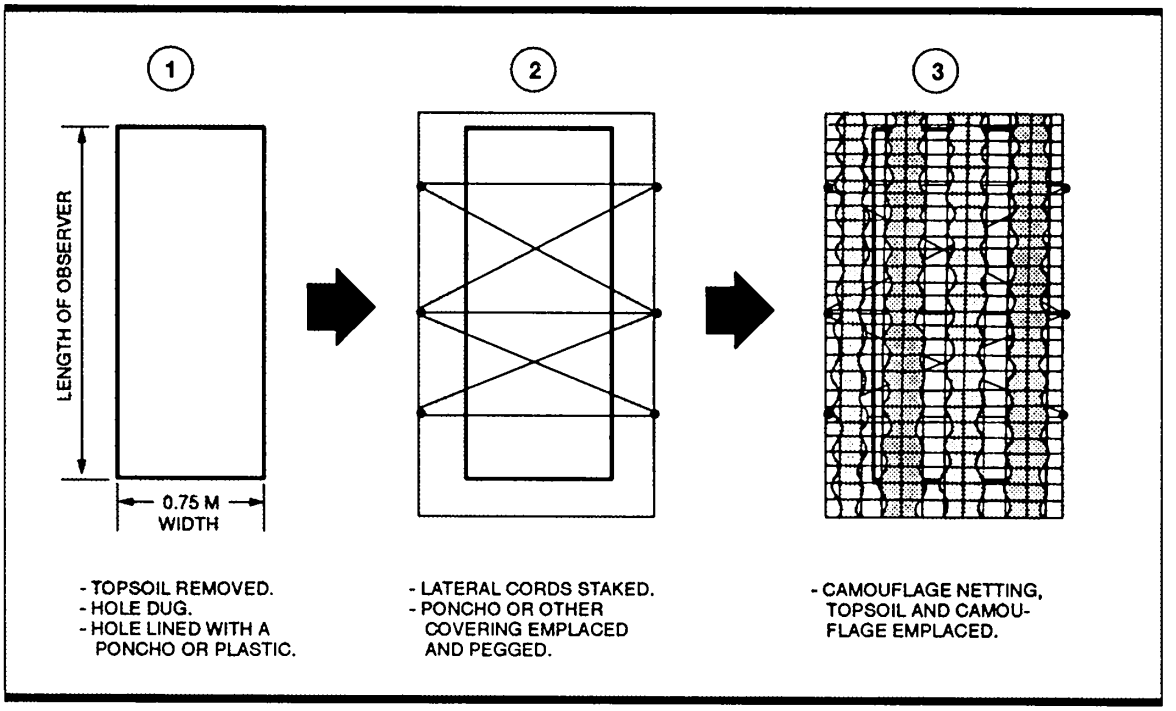


Figure A-5. Scrape plan example.

Tent-type site. Larger than a spider hole, this site is constructed for more than one observer. Supports for the overhead cover are made from a variety of material. Branches, aluminum conduit, parachute suspension line, or fiberglass rods all work well as a frame for the cover. A slight arch in the cover multiplies the available space on the inside of the site. The observer avoids grossly breaking the ground plane with the apex of the site. (See Figure A-6.)

Underground Site. The safest type of observation site for the observer to use is the underground site. The complexity of design and the effort required to construct the site are the primary detractors. When using light equipment such as shovels and entrenching tools, underground sites can only be constructed in loose soils. Soil type is a very important planning consideration that must not be overlooked during mission preparation.

Bunker-type site. This site requires extensive construction time and material to complete. The observer can construct the underground bunker-type site using a prefabricated kit. This kit includes the tools needed to excavate and cut local materials such as trees and logs. The kit also contains plastic sheeting for waterproofing the roof, walls, and floor. The sheeting can also be used to reinforce loose soil in the site. However, depending on the soil in the area, sandbags are often required to shore up the sides of the site. Also, sandbags lessen the accumulation of condensation produced when plastic sheeting is used. (See Figure A-7.)

Caves. Caves can provide the observer with a ready-made observation site. However, caves present special problems. First, caves attract attention. They are often shown on maps or are known to the local populace. Locals often use caves for shelter and sometimes for storage. Caves also attract animals. Bats, birds, snakes, and larger animals use caves for shelter. The presence of these animals presents medical risks to the SFOD members. Also, early warning devices may be activated and attract the attention of local threat forces. Using caves increases the chance of discovery and is avoided in all but emergency situations.

Construction Techniques

Several construction techniques are common to all observation and surveillance sites. These techniques are included in SOPs and practiced during normal training.

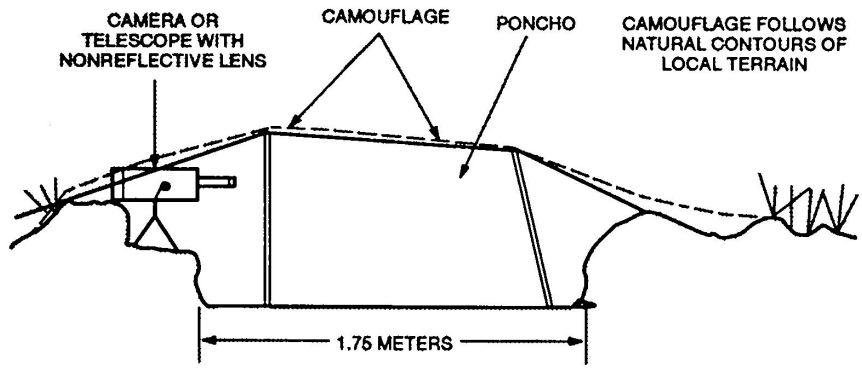


Figure A-6. Tent-type observation site.

Dirt Removal. The primary problem in constructing any site is the removal of excess dirt. Excavated soil expands in volume. In dry climates, the subsurface soil contains the most water. This water content causes the soil to be a different color. This soil must be camouflaged. The SFOD constructs underground sites before the early morning dew develops. Discarding excess soil before the dew sets in aids in the camouflage process. The SFOD also considers the effect of the sun drying out the excess soil. This dried soil may need to be recamouflaged. The main technique for camouflaging soil involves the use of plastic sheeting or a poncho. The steps are as follows:

- Lay out the sheeting alongside the site position.
- Place the topsoil to one side of the sheeting. Remember that the topsoil only extends a few centimeters below the surface. Save as much of the vegetation as possible. (See Vegetation, page A-14.)
- Dig out the remaining soil. Do not mix the topsoil with subsoil from hole.
- Fill sandbags with the (loose) soil dug from the hole and use them to reinforce the sides of the site.
- Fill surrounding depressions, ruts, or ditches with the remaining excess soil. If this procedure is not possible, spread the soil lightly on the surface in an area away from the site. Avoid putting the excess soil in creeks or streams that may wash the dirt down the waterway and attract unwanted attention.
- After the overhead cover is constructed and waterproofed, replace the topsoil. Place vegetation, leaves, deadfall, or other local materials about the area to complete the camouflage of the site.
- The final step in the process is to recover the sheeting used to contain the soil. Check the vegetation under the sheeting to ensure that it was not matted down under the weight of the soil. If matting has occurred, take the time to brush it with a branch to return it to its natural state.
- As time passes, continually check the vegetation and soil around the site to ensure that they appear natural. Loose soil often falls through small holes and results in a strange-looking, funnel-shaped hole. Check vegetation to ensure it blends with the surrounding area. Remove or replace dead vegetation.

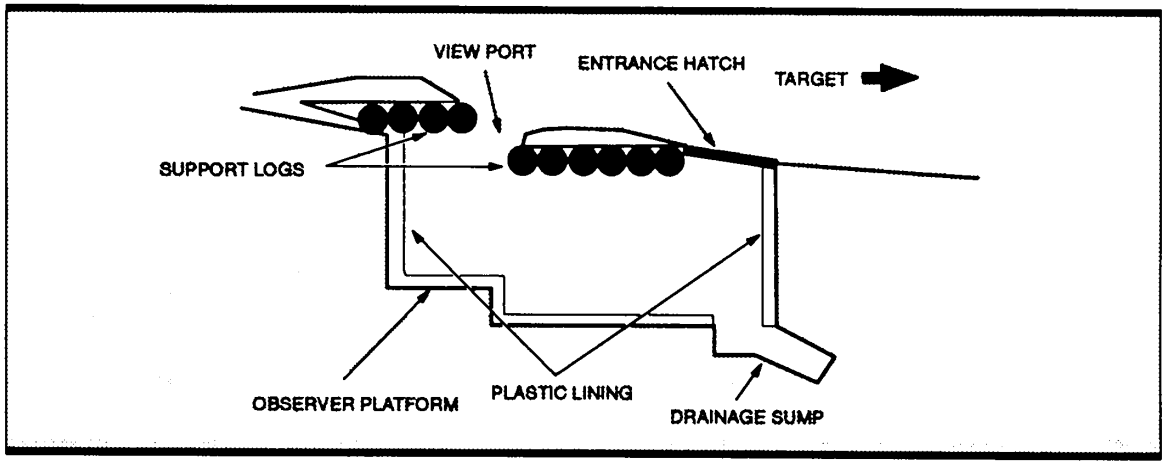


Figure A-7. Underground observation site plan.

Vegetation. When applying the B in the BLUES acronym to the SR site, remember vegetation is critical. Replanting and watering vegetation during initial site construction can eliminate the need to continually replace wilted plants.

Grasses. When removing topsoil, save the grass. Remove the grass in clumps by cutting a circle about 5 to 15 centimeters around the section to be saved with an entrenching tool or shovel, then pry the roots and soil up from the bottom. When replacing the grass around the site, pattern the placement after the natural design. Shake the grass slightly to loosen the roots, then replace at ground level. If water is available, a small amount placed on the grass will lessen the shock of replanting and extend the life of the camouflage.

Plants and bushes. Medium-sized plants or bushes will aid the security of the site. Not only will the plants add to the camouflage of the site, but they will also discourage vehicle and foot movements over the top of the site. The main disadvantage to using plants on top of the site is that the plants may die or fall over due to the shallow depth of the overhead cover. Also, if close quarters battle develops between a member of the SFOD moving outside the site and a threat element, the threat may take cover behind the plant and thus discover the actual location of the site.

Deadfall. Deadfall can restrict movement in much the same way as the plants and bushes discussed above. However, the use of deadfall as part of the overall camouflage effort presents several disadvantages. The main disadvantage is that in most regions of the world, deadfall is used for home heating, cooking, and construction. If the site has this fuel near it, the risk of discovery is increased. The SFOD members have limited options available to them if discovered by a — nonhostile civilian: emergency exfiltration or activation of the E&E plan. Either course of action will result in the mission being terminated. Cover from small arms fire is very limited when using deadfall. Most trees rot quickly when on the ground. Modern small arms fire will easily pass through these rotten trees. For this reason, the SFOD avoids using deadfall for cover. If it must be used, it is reinforced with dirt.

Sidewall Support. Depending on the soil condition in the AO, the sidewall of the site may require some type of shoring or support to prevent cave-ins. The SFOD can use a variety of material for support of the walls. Local timber, branches, deadfall, plastic sheeting, and ponchos ail work well. However, the primary means for supporting the sides is by using sandbags. These lightweight bags serve a variety of uses and conform to almost any shape required. The exact number of bags required depends on the size and overall design of the site. The SFOD determines this variable by practicing the construction of the proposed site. After the SFOD has tested the design and determined the number of required bags, it figures a 10 percent overage into the packing list. The few extra bags add flexibility for unforeseen factors such as replacements for damaged bags. The bags can also be used for transportation purposes. When cross bracing sandbagged wails, the SFOD must use freshly cut green timber or something prefabricated, such as PVC pipe, conduit, or other like items. Examples of cross bracing and revetments can be found in FM 5-34.

Observation Site Kits. When possible, the SFOD assembles prefabricated kits to aid in the construction of the required site. These kits need not be taken into the

operational area but are assembled as a stockpile. This stockpile can then be drawn upon for mission-specific equipment during isolation. Some of the items in these kits are—

- Schedule 80 PVC pipe, elbows, straight connectors, 3- and 4-way connectors, and PVC cement. This strong, lightweight material can be formed into a multitude of shapes and designs. It can be used to form the frame of the overhead cover or to form cross bracing.
- Parachute suspension line. This material serves many uses. It can also be interwoven to produce a frame for overhead cover.
- Sandbags.
- Assorted tapes, cords, and ropes.
- Plastic Zip-Lot bags. These items can be used for general storage.
- 0.5-meter x 0.5-meter squares of 1-centimeter plywood. This lightweight material is excellent for constructing overhead cover, platforms for use in trees, and insulation when operating on ice and snow. The squares are painted to match the terrain in which they are used.
- Plastic sheeting. Heavy-gauge plastic sheeting fills many roles. If plastic sheeting is not available, the heavy-duty plastic bags used to cover pallets work well.
- Hand tools. (D-handle shovels, hack saws, hammers, small bow saws, and like items.)
- Plastic or aluminum tent stakes. These items save time during construction of the site.
- Canvas and camouflage netting.
- Plastic buckets with formaldehyde.
- Mirrors or periscopes.

COMMUNICATIONS SITE

Like the observation and surveillance site, the communications site can be a fixed position or part of a patrol. If the communications site is to be a fixed position, the SFOD may select and construct it in the same basic fashion as it does an observation and surveillance site. This site provides HP, satellite, and other types of communications between the SFOD and its SFOB. Conducting SR communications between the SFOD and its supporting SFOB is critical. SFODs are required to pass timely information to the SFOB and to receive instructions and information. Communications between the communications site and outlying sites may be by buried wire, low-power FM radios with directional antennas, or messenger. Based on METT-T factors, a communications site is routinely separate for technical and security reasons. The advantages of a separate communications site are the reduced risk of detection of direction and location through radio direction finding (DF) and reduced number of personnel at any one location. The disadvantage of a separate communications site is the increased risk of detecting messengers moving between sites (Figure A-8, page A-16).

SURVEILLANCE SITE OCCUPATION

Occupation of the surveillance site is basically the same as an occupation of a patrol base (see TC 31-29 for information on patrol bases). The main difference is that the main body of the SFOD may not occupy the site. Part of the element may remain in the ORP and establish communications, cover the route taken into the ORP, or gather the local material needed to construct the site. The primary or first shift of observers moves to the selected site only after the SFOD leader has established security. After an appropriate listening halt has detected no activity in the area, SFOD members may begin work on the site. After the construction is completed, all SFOD members should know the exact location of the site, routes to and from the site, and time of shift changes. Before the SFOD leader returns to the ORP, he reviews the completed site from the threat side to ensure the site is completely camouflaged. He then obscures all signs of occupation as he and the security element return to the ORP.

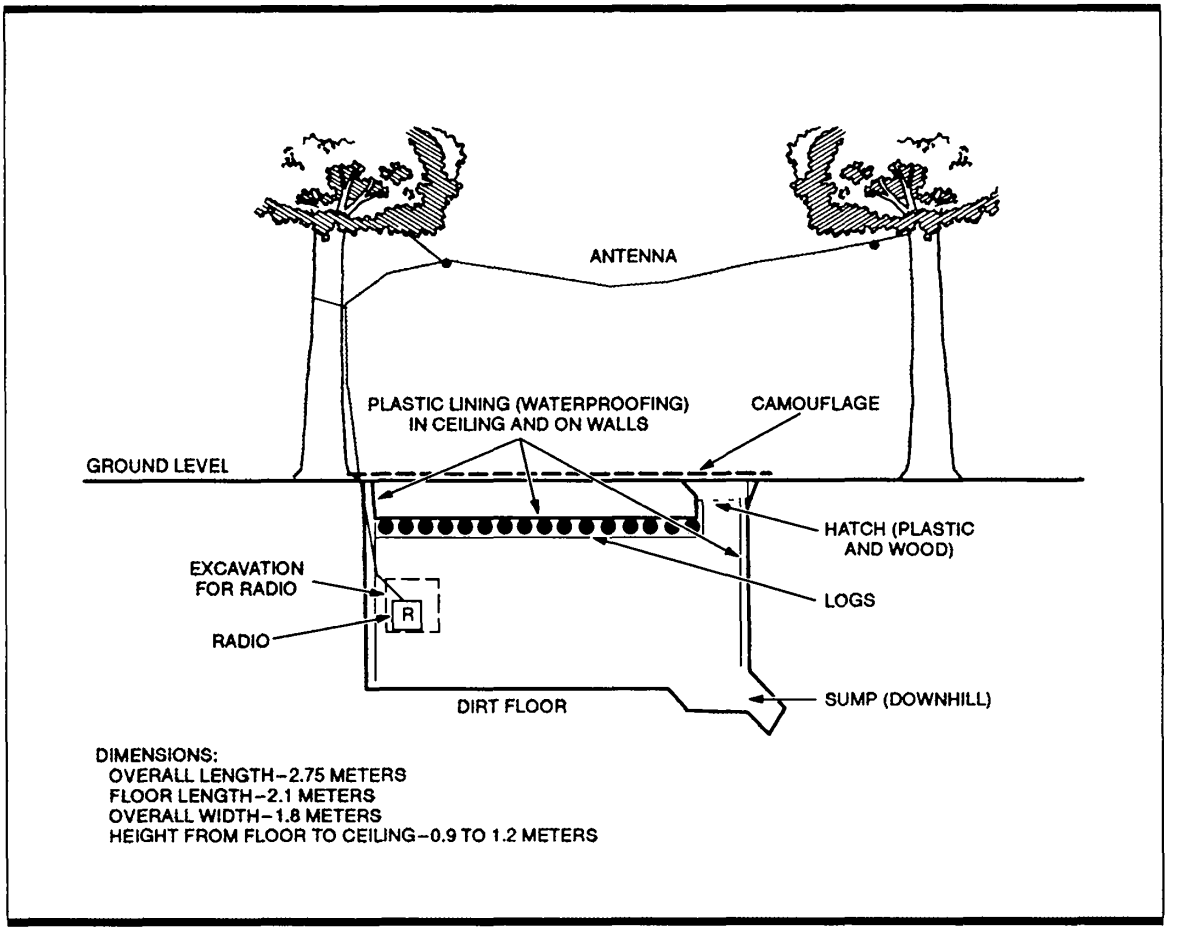


Figure A-8. Communications site.

FM 34-45

Tactics, Techniques, and Procedures

ELECTRONIC ATTACK

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

a baseline for future missions. In an environment rich with signals, it is imperative that EA is delivered with precision and overpowering force. Figure 6-1 shows an example of using ingress routes into division or brigade AOs.

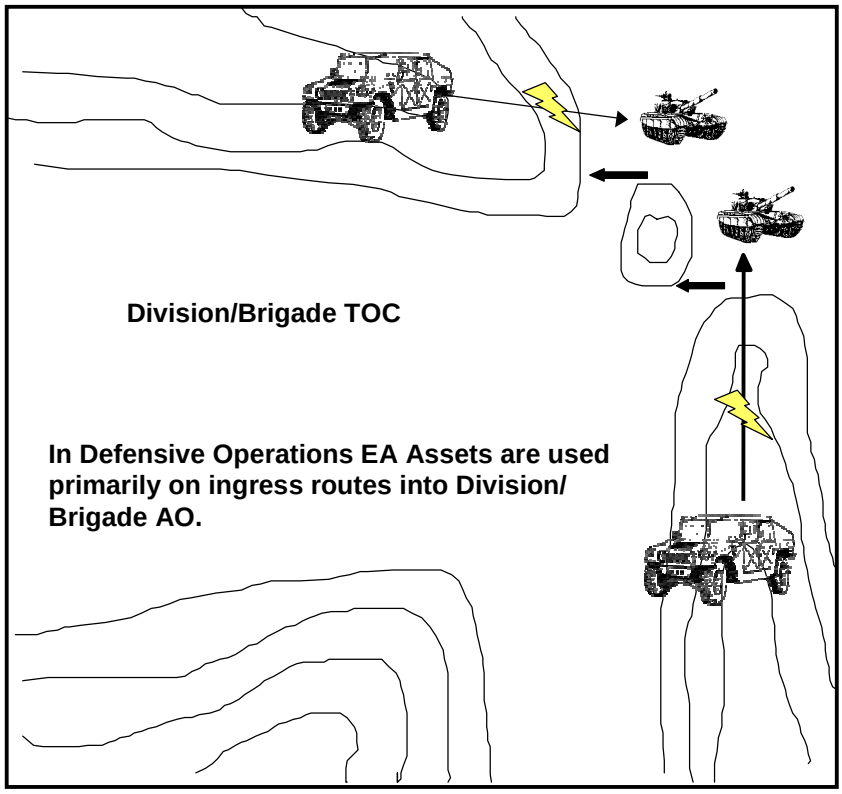


Figure 6-1. Division or Brigade TOCs

CONDUCT ELECTRONIC ATTACK

6-5. This operation has three functions. **Acquire target**, **reappraise and apply jamming equation**, and **jam target**.

ACQUIRE TARGET

6-6. This function has three steps: **Confirm target technical parameters**, **monitor target frequency**, and **confirm target acquisition**.

Confirm Target Technical Parameters

6-7. This step consists of three tasks:

- Confirm target frequency. The team leader will confirm with the TA team or POC the specific target frequency and ensure if jump frequencies were used that they were provided with jump sequence and correct jump frequencies.

- Confirm spectrum scan segments. The team leader will next use the scan function on the system to determine the exact frequency. This process is done because recalibration of a system is rare and the frequency may not correspond exactly.
- Confirm continued monitoring of target. The operator or team leader will confirm with the TA team the continued monitoring of targets.

Monitor Target Frequency

6-8. This step has three interrelated steps:

- Monitor designated frequency. The operator will monitor the frequency.
- Monitor designated scan sectors. The operator will monitor the particular sectors to ensure the system is still on target for the exact frequency.
- Revisit target frequency. The operator will periodically check on the target. How often the asset revisits the target is determined by the number of targets and the SIGINT team.

Confirm Target Acquisition

6-9. This step has four sequential steps:

- Acquire signal. This task is covered in the previous section.
- Identify signal. The operator will identify the particular signals with data passed by the SIGINT team.
- Confirm signal is designated target. The operator will use this data to confirm that the target is the same target passed by the SIGINT team. Examples of this confirmation would be callsigns, jargon, language, and essential elements of information.
- Confirm signal is preplanned target or target of opportunity. The operator will confirm that the target is either a preplanned target or a target of opportunity. This task is the last confirmation that the target is the correct target.

REAPPRAISE AND APPLY JAMMING EQUATION

6-10. This function will be performed by the SIGINT team to ensure that the EA asset can acquire the target and the target will be within range of the EA asset. The jamming equation will give the SIGINT team a range of each EA system with regard to particular emitters and receivers. Doctrine and equipment capabilities dictate quick and overpowering EA attack; therefore, this equation is not used for minimum power. An example of this are targets of opportunity. The EA team will not have the time to perform the equation and fine-tune the EA asset to hit the target with minimum power (minimize the asset's signature). The requirement for this technique is no longer valid because these assets deliver quick overpowering attacks.

JAM TARGET

6-11. This function has four steps.

Review Jamming Control

6-12. This step will ensure that there is a "stop jam" frequency being monitored by the system.

Program Jamming Power Output

6-13. This step will pass from the tasker to the jammer the power output for the system. This step is usually bypassed with the assumption that maximum power for precise overpowering EA will be used.

Jam Target Using Predetermined Techniques

6-14. This step will direct the EA system in the particular techniques to use. There are four basic techniques: **deception**, **jamming**, **masking**, and **DE**.

6-15. **Deception.** EM deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information to an enemy or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. There are three primary types of EM deception:

- Manipulative EM deception, which involves actions to eliminate revealing or to convey misleading EM telltale indicators that may be used by hostile forces.
- Simulative EM deception, which involves actions to simulate friendly, notional, or actual capabilities to mislead enemy forces.
- Imitative EM deception, which introduces EM energy into enemy systems that imitate enemy emissions.

6-16. **Jamming**. EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the purpose of preventing or reducing an enemy's effective use of the EM spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. Jamming falls into two categories, voice and digital (analog) data. Communications jamming is targeted against hostile voice systems for multiple purposes:

- To introduce delays into the enemy's C^2 system that allows the friendly commander to fully exploit his options.
- To delay hostile time-sensitive information until it is no longer useful.
- To force the enemy (in conjunction with ES) into actions that are useful to friendly operations. There are three primary types of EM jamming:

An example of EA forcing the enemy into action useful to friendly operations out of encrypted communications through jamming allows ES to gather intelligence from this otherwise secure net and further develops an intelligence baseline.

  - Spot Jamming. Spot jamming may be directed at a single frequency or multiple frequency through sequential spot jamming and involves jamming various frequencies one at a time in

sequence. Simultaneous multispot jamming involves jamming several frequencies at the same time. In both spot and sequential spot jamming, the full power of the jammer is directed against one frequency at a time, increasing the effectiveness and range of jammer. Spot jamming is less likely to interfere with friendly communications because receivers and transmitters can easily avoid it by slightly changing (detuning) the frequency they are receiving.

- Sweep Jamming. In sweep jamming, the jammer goes through a frequency range, then repeats the sweep continuously. All frequencies in the range are jammed. Friendly frequencies may be affected unless protected by the Joint Restricted Frequency List (JRFL).
- Barrage Jamming. Barrage jamming, unlike spot jamming, simultaneously spreads the jammer's power over a larger portion of the frequency spectrum, thereby reducing radiated power directed at any single target frequency. Barrage jamming is similar to sweep jamming, since all frequencies are jammed within the targeted portion of the spectrum.

6-17. **Masking**. Electronic masking is the controlled radiation of EM energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy ES without significantly degrading the operation of friendly systems.

6-18. **Directed Energy.** DE is an umbrella term covering technologies that relate to the production of a beam of concentrated EM energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to damage or destroy enemy equipment facilities and personnel. Directed energy warfare (DEW) is military action involving the use of DE weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel; or to determine, exploit, reduce, or prevent hostile use of EM spectrum through damage, destruction, and disruption. (See Appendix A for more information on DE in EW.)

Report Inability to Locate Target

6-19. The operator reports the inability to locate the target and therefore to queue ES assets to search for the target or to pass targets to other EA assets.

JUMPING EA ASSETS AFTER EA MISSIONS

6-20. Dependent upon METT-TC, the commander must review the advantages and disadvantages of moving EA systems after EA missions. This decision becomes more critical as threat technology increases.

- Advantages: Jumping systems after each mission increases survivability due to the strong EM signature produced during jamming missions. These signatures are easily located if in the VHF range. When located, ES assets can DF these signatures and provide support

to targeting for lethal fires and various other means to destroy the EA asset.

- Disadvantages: Jumping systems after each mission will dramatically decrease the amount of EA missions which can be accomplished. The tear-down, set-up, and movement time will use up critical resources, specifically time. Due to the necessity of locating EA assets near the FLOT, movement will also expose systems to threat forces in the area of movement. Therefore, the decision to move is balanced against missions and resources.

REPORT ELECTRONIC ATTACK RESULTS

6-21. This operation has two functions: **determine effectiveness** and **prepare and transmit EA report**.

DETERMINE EFFECTIVENESS

6-22. This function has three steps.

Determine Degree of Disruption to Threat Communications

6-23. This step has four tasks:

- Monitor target reaction. In this task the team leader will record and analyze the reaction of the target. The team leader records the specific reaction of enemy forces with the support of an ES asset such as communication phrases (for example, "we are being jammed" "say again," "repeat all after,") or no verbal recognition of voice communications or contradictory acknowledgement. Contradictory acknowledgment (for example, "go to assembly area Bravo" when the original message was assembly area Golf). These statements would mark the conclusion of a successful EA mission.
- Estimate degree of degradation to maneuver. The team leader would once again listen for phrases, which would provide information. The team leader will also look for phrases that indicate delay, disruption, and diversion of maneuver elements (for example, "Mike 14 you are off line," "Mike 14 move back into formation.") If these phrases are repeated to several different units in the element, the EA is effective.
- Estimate degree of degradation of fires. This task can be analyzed if the target is a voice net. With the digital artillery nets, the team leader will not be able to assess effectiveness, but ES systems will be able to monitor the net to see if the jamming is overpowering the signal to the receiver. Also, assessment of the battlefield will reveal if the enemy forces initiated any artillery missions. A forward observer (FO) calling for fire and adjusting fire—
  - Has to repeat coordinate.
  - Is delayed passing adjustments.
  - Adjustments are delayed in firing.

6-24. The team leader will look to see if the mission is performed and the degree of effectiveness. If multiple adjustments over several minutes are not made and the unit moves out of the area, but the FO cannot walk the rounds onto the unit, the EA mission is successful.

- Estimate degree of degradation. The team leader performs this task. This effectiveness is determined by multiple means. Voice analysis identifies similar phrases in the monitoring of target reaction. Also, the team leader will look for indicators that actions are not followed or performed. Another way to estimate degradation is for the ES assets to report the splintering of the net. Throughout these tasks, the ES systems must support the EA personnel orienting the EA systems. It is also critical to support EA assets for effectiveness. For EA systems using encrypted communications channels, the ES system will monitor the net to see if EA overpowers the system and if the voice net drops into the "red." These actions are clear indications of the effectiveness of EA. Many nets will assume bad encryption and simply go "red" to communicate. If this happens, EA may cease and ES begins to gather intelligence until the SIGINT team tasks the EA team to reattack the target.

Prepare EA Rating Table

6-25. This step has two tasks.

- Estimate mission success. The team leader, in conjunction with the ES assets, performs this task to estimate the degree of degradation of communication and noncommunications nets. This will determine the success of mission.
- Describe threat reaction to EA. This reaction is recorded in the determine degree of disruption to threat communications. These reactions are compiled by the tasking agency to give overall enemy reaction to EA.

Prepare to Continue Mission or Begin New Mission

6-26. The SIGINT team will decide whether to continue the mission based upon the EW annex. If the mission is ineffective, the SIGINT team may task the EA asset to employ a different technique or it may pass the mission to other EA assets. If the mission is successful, a determination will be made if the net is still a viable target or to move onto another mission.

PREPARE AND TRANSMIT EA REPORT

6-27. This function has two steps. These steps conclude DELIVER, although this is truly a continuous cycle.

- Transmit effectiveness report. A MAER is sent by the team leader to the tasker to report the overall effectiveness and status (a basic summary) of the missions performed by the EA asset. The MAER—
  - Will queue the SIGINT team for additional missions and any specific reports needed before new missions are begun.

- Will also provide details on the target, target reaction, mission success, and techniques employed.
- Is not only a report on the effectiveness of EA but also upon the reaction of enemy forces to particular techniques.
- Is used to build a database on the use of EA against specific units and their specific reactions and provide EA assets and EWOs more concrete expectations when delivering EA.

- Summarize significant EA mission technical parameters. These technical parameters summarize the frequencies and power used on specific targets.

SUMMARIZE STATUS OF ELECTRONIC ATTACK ASSETS

6-28. This task will provide a basic system status report. The EA system will send a multiple assets status report (MASTR) to the SIGINT team detailing the team status. This will provide the exact status of each EA asset to include the fuel, water, food, and ammunition. When combined with the system status, they give the SIGINT team a complete understanding of the system and its ability to perform additional missions.

Chapter 7

ASSESS

EW operators constantly evaluate the effectiveness of EA missions and report this information to the supported unit. The supported unit in turn incorporates these EA effectiveness reports into their combat assessment of the targeting effort. The combat assessment is the final function in the targeting process. The assessment represents the staff's determination of the effects of fires (lethal and nonlethal) on the enemy and whether these effects are accomplishing the commander's targeting objectives. The combat assessment forms the basis for the staff's reattack recommendations to the commander and future weapon system selection and employment. Assessing EA begins with the operators.

OPERATOR EVALUATION

7-1. It is important for the operator to evaluate EA effectiveness based upon the desired effects contained in the attack guidance. This technique provides the operator with a quantifiable measure of EA effectiveness. The use of percentages or other numerical formulas at the operator level are not accurate and add little to the assessment of EA effectiveness on the battlefield. The EA system operator and operators of the supporting ES systems execute the following steps to evaluate the effectiveness of EA missions.

RECORD JAMMING EFFECTIVENESS

7-2. During jamming missions, ES operators monitor the target to determine if the jamming is overpowering the signal to the receiver and affecting the target operator's ability to communicate.

RECORD EFFECTS ON THE TARGET SIGNAL

7-3. This is particularly important when attacking targets such as encrypted voice and data networks. EA and ES operators cannot access or exploit the internals of these communications systems and must judge the effects of jamming on the signal itself. Understanding the effects of the jamming signal on the target signal is also important when using EA and ES operators that are untrained in the target language. If the jamming is overpowering the signal, then the ES system will hear the noise of the EA system override that of the target transmitting station. The operator will also see a "spike" on the oscilloscope when the EA system signal is active. If these indicators occur, then the EA operator can assume the attack is effectively disrupting the target's ability to communicate.

RECORD OPERATOR COMMENTS

7-4. Listen for operator comments about difficulty communicating or executing operations. Phrases such as "I can't hear you, say again," "we are being jammed," and "repeat all after" indicate that the jamming power and technique are disrupting communications. Record instances where the operator repeats movement instructions, firing data, and situation reports. Note incidents where operators do not acknowledge a transmission and messages or give contradictory acknowledgments. An example of a contradictory acknowledgement would be when the operator confirms "assembly area Bravo" when the original message was "assembly area Golf." Additionally, the operator should listen for changes in attitude, rate of speech, and use of obscenities that reflect the operator's emotional response to the effects of EA. Operator comments provide important information about the EA technique employed and whether the EA mission achieved the targeting objective.

RECORD COUNTERMEASURES TO JAMMING

7-5. The ability of the operator to recognize and react to EA varies based on his training, experience, and discipline. An inexperienced operator may attribute the noise or broken communications to nature or equipment rather than to EA. This type of operator will attempt to work through the EA rather than to take countermeasures such as switching to an alternate frequency or mode of communications. The more experienced and trained operator will recognize EA and initiate some form of countermeasure to defeat or minimize the effects of EA. Noting how long it takes the operator to recognize EA and to take action are important pieces of information for future EA mission on the target or similar targets.

DETERMINE JAMMING EFFECTIVENESS

7-6. The level of accuracy in this subjective evaluation depends upon the training and experience of the EA operator. The assessment begins with the operator reviewing the EA guidance contained in the tasking message or OPORD. The operator considers the jamming mission successful if the mission occurred on time, against the correct target, and achieved the desired EA targeting effect.

REPORT JAMMING EFFECTIVENESS

7-7. The EA operator provides a JER to the TA team, which in turn compiles these reports into a MAER for the SIGINT team that addresses the effectiveness of the mission. The SIGINT team will forward this information in a signal summary (SIGSUM) to the EWO for MEA. This report gives details on the target, target reaction, and techniques employed. This report is not only a report on the effectiveness of jamming but also on the effectiveness of the particular techniques against a target type. Targeting and planning personnel use this information to ensure EA assets are employed to their fullest potential against appropriate targets.

REPORT DECEPTION EFFECTIVENESS

7-8. Assessing the effectiveness of deception occurs at the ACE as they fuse intelligence to discern the threat's reaction to the deception operation. Deception assessment occurs seldomly at the operator level. Indicators for operators of a successful deception operation are threat forces attempting to communicate, to gather data, and to coordinate movement if using imitative deception. (See Appendix D for more information on electronic deception.)

UNIT COMBAT ASSESSMENT

7-9. The unit staff builds the combat assessment from BDA and MEA. BDA describes the effects of targeting (lethal and nonlethal fires) on the target and forms the basis for reattack recommendations. MEA addresses the effectiveness of munitions, weapons systems, and tactics. Together, BDA and MEA help the unit understand the impact of the current FS plan on the threat and improve the targeting effort in future operations.

BATTLE DAMAGE ASSESSMENT

7-10. The G2 is primarily responsible for developing the BDA within the unit staff. During DECIDE, the G2 assists the commander in setting BDA requirements for HPTs. The G2 incorporates these BDA-related PIR into the collection plan and orders to subordinate units. This supports the timely collection and reporting of BDA information to the G2. For EA missions, this ensures ES systems are tasked to collect and report on the effectiveness of EA missions.

7-11. In addition to intelligence reports and operator evaluation, the G2 also uses target development and FS planning products to develop the BDA. The DECIDE phase products provide the G2 with the target descriptions, attack rationale, and desired effects that the targeting team used to develop the HPTL and concept of fires. The G2 should refer to the following documents during BDA development. The staff should also update these and other documents (for example, situation template, target synchronization matrix, collection plan, and FS plan) based on the results of the BDA.

- Concept of fires provides the task, purpose, method, and desired effects required to support the commander's scheme of maneuver.
- HPTL provides a mechanism for prioritizing the analysis effort with the targeting priorities. The EA effectiveness report should include the target number to assist in associating reports to targets.
- Target spreadsheet provides the analytic yardstick for comparing the desired effect contained in the concept of fires and HPLT with the actual effects. In the case of EA targets, situation templates reflecting the threat EOB and critical nodes should be present in the spreadsheet or as a separate electronic preparation of the battlefield product.

7-12. With the raw data such as the EA effectiveness report and reference material in hand, the G2 begins the task of sorting and analyzing the data to develop an all-source intelligence BDA of the effects on the target. To further aid in this task, each BDA is broken down into three components. Each component allows the G2 to scrutinize and record the effects on the target

from a number of perspectives. These three different assessments also require different sensors, analytical elements, and timelines. They are not necessarily subcomponents of each BDA report. The four components are physical damage assessment (PDA), functional damage assessment (FDA), target system assessment (TSA), and MEA.

Physical Damage Assessment

7-13. PDA estimates the quantitative extent of physical damage through munition blast, fragmentation, and/or fire damage effects to a target. This assessment is based on observed or interpreted damage. While EA is not traditionally thought of as physical damage, the EWO can develop an immediate assessment of the effectiveness of EA through "observed or interpreted damage."

7-14. **Observed Damage.** Much like lethal fires, EA can be either observed or unobserved nonlethal fire. Observed EA requires an ES asset to "observe" or monitor the effects of the EA on the frequency of the system under attack. The EWO must identify EA targets requiring ES collection during the DECIDE function of the targeting process. If the requirement becomes a PIR, the collection manager will then request or task support for monitoring the EA target. The ES asset will then monitor the target and provide feedback to the EA asset on the effects of the attack. At the end of the EA mission, the EA and ES will send a MAER to the EWO and collection manager on the results of the mission.

7-15. **Interpreted Damage.** If an ES asset cannot monitor the EA mission, then the operator must interpret the effectiveness of the attack based on the asset's proximity to the target, ability to acquire the target, technical factors (for example, signal-to-noise ratios), and operator experience. The EA asset and SIGINT team cannot quantitatively interpret the effectiveness of unobserved EA. Unlike the physical signs of the effects of lethal fires, the effects of unobserved EA cannot be evaluated based on post-strike reconnaissance.

Functional Damage Assessment

7-16. The FDA estimates the degree of degradation caused by EA against the target compared to the operational objective established against the target. This assessment is inferred on the basis of all-source intelligence and includes an estimate of the time needed to replace the target function. An FDA is a temporary assessment (compared to TSA) used for specific missions.

Target System Assessment

7-17. The TSA is a broad assessment of the overall impact and effectiveness of all types of attack against an entire target system's capability (for example, threat air defense systems). It may also be applied against threat unit combat effectiveness. A TSA may also look at subdivisions of the system compared to the commander's stated operational objectives. It is a relatively permanent assessment (compared to an FDA) that will be used for more than one mission.

Munitions Effects Assessment

7-18. The FS staff (or G3/S3 through the targeting team in accordance with FM 6-20-10) is responsible for developing the MEA concurrently and collaboratively with the BDA. For EA systems, the team depends upon the information in the EA effectiveness report to determine the effectiveness of the EA system against a particular target. The assessment forms the basis of recommendations for changes to increase the effectiveness of the following:

- EA tactics (system selection, positioning, deployment, and redeployment).
- EA techniques (spot jamming, imitative deception, intrusion).
- EA procedures (tasking and reporting channels, ES and EA system tip-off, technical data).
- EA systems (system capability, operator qualifications, mobility).

REATTACK RECOMMENDATION

7-19. Based on the BDA, the staff determines if the targeting objectives were met and if reattack is necessary. MEA helps the staff to select the best weapon system to execute the reattack. Both BDA and MEA give the staff the information needed to develop a complete reattack recommendation for the commander. In some cases, BDA and MEA may indicate that EA is not capable of meeting the targeting objective. The combat assessment process allows the staff to—

- Recognize that shortcoming in the FS plan.
- Select an alternate weapon system (lethal or nonlethal).
- Reattack the target.
- Achieve the targeting and operational objectives. (See Joint Publication 2-01.1 and FM 6-20-10 for more information on combat assessment.)

7-20. See Appendixes E, F, and G for more information on target reports, DS, and military operations on urbanized terrain (MOUT).

Appendix A

The Electromagnetic Environment

EM energy is both a natural and manmade occurrence. This energy, in the form of EM radiation, is made up of oscillating electric and magnetic fields and is propagated at the speed of light. EM radiation is measured by the frequency of its wave pattern's repetition with a set unit of time. The standard term for the measurement of EM radiation is the hertz (Hz), the number of repetitions (cycles) per second. The term **"**electromagnetic spectrum**"** refers to the range of frequencies of EM radiation from zero to infinity. The spectrum is divided into 26 alphabetically designated bands.

MILITARY ELECTROMAGNETIC SPECTRUM

A-1. Figure A-1 shows the principal military segment of the EM spectrum with the corresponding EW frequency bands and radar designations and why there is occasionally confusion when discussing frequency bands, which share names in different designation systems. The EME is the resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted EM emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. The EME is the sum of—

- EM interference.
- EM pulse.
- Hazards of EM radiation to personnel, ordnance, and volatile materials.
- Natural phenomena effects of lightning and precipitation static (p-static).

A-2. P-static is created by charged precipitation particles that strike antennas and gradually charge the antenna, which ultimately discharges across the insulator, causing a burst of static.

MILITARY OPERATIONS AND ELECTROMAGNETIC ENVIRONMENT

A-3. The impact of the EME upon the operational capability of military forces, equipment, systems, and platforms is referred to as EME effects. EME effects encompass all EM disciplines, including—

- EM compatibility (EMC) and EM interference (EMI).
- EP.
- Hazards of EM radiation to personnel, ordnance (HERO).
- Volatile materials such as fuels.

- Natural phenomena effects of lightning and p-static.

A-4. Equipment and systems which operate on the principles of electromagnetism are characterized by electromagnetic vulnerability which cause them to suffer a definite degradation (incapability to perform the designated mission).

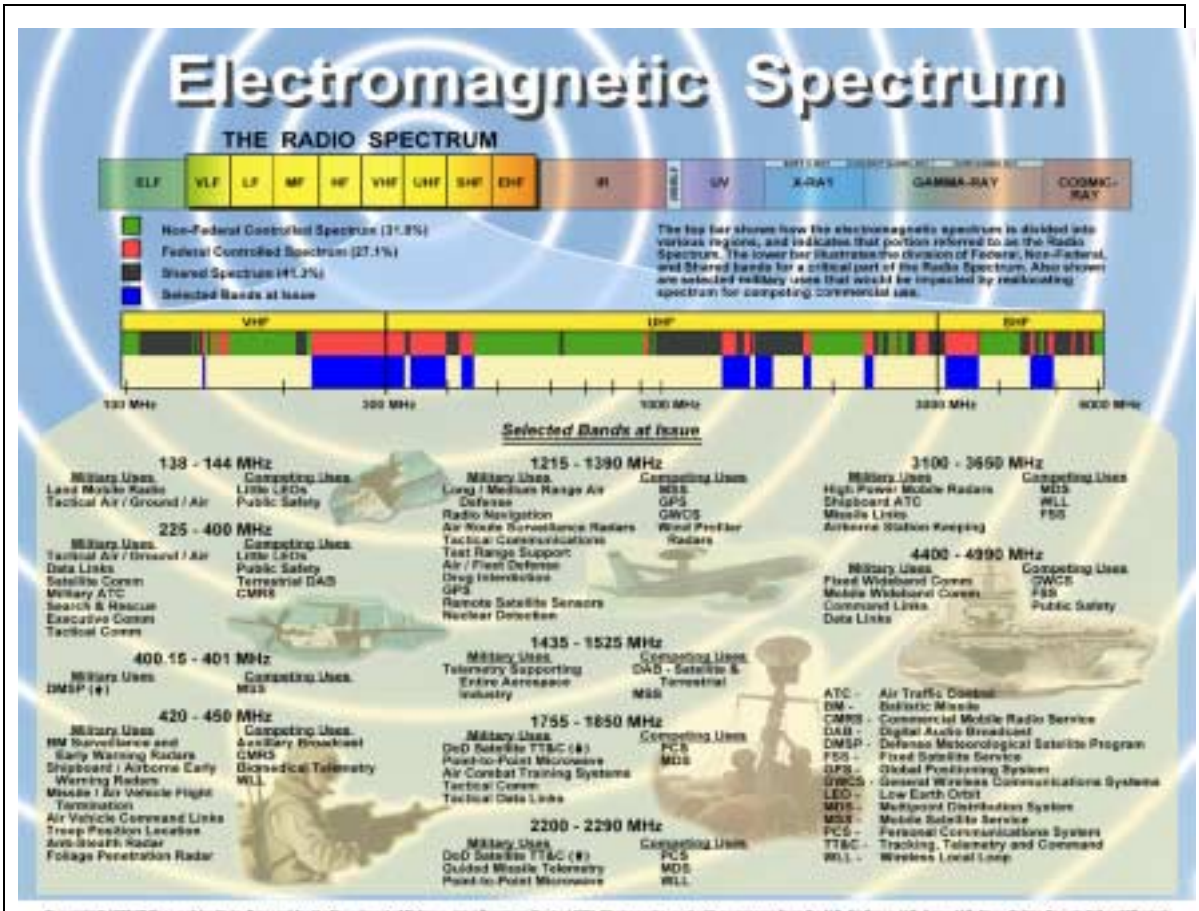


Figure A-1. Electromagnetic Spectrum

DIRECTED ENERGY IN EW

A-5. DE includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the EM spectrum. Possible applications include lasers, RF weapons, and particle beam weapons. As the development of DEW evolves, TTP must also evolve to ensure their safe, effective employment. Although some DE applications will easily fit into traditional EW roles, others will not. For example, in EW terms—

- A laser designed to blind or disrupt optical sensors is ES.

- A laser-warning receiver designed to detect and analyze a laser signal is ES.
- A visor or goggle designed to filter out the harmful wavelength of laser light is EP.

A-6. The potential for the threat's use of destructive DE weapons and other destructive RF weapons is also growing. Intelligence assets must be tasked to collect information about this threat, and joint planning must include the development of operational procedures and COAs to mitigate the effects on these weapons.

PRINCIPAL ELECTRONIC WARFARE ACTIVITIES

A-7. The principal activities used in EW have been developed over time to exploit the opportunities and vulnerabilities, which are inherent in the physics of EM energy. Although new equipment and new tactics continue to be developed, the physics of EM energy remains constant. This physical constant is the reason that the basic activities of EW remain effective despite changes in hardware and tactics. The principal activities used in EW follow.

ELECTROMAGNETIC COMPATIBILITY

A-8. EMC is the ability of systems, equipment, and devices that use the EM spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of EM radiation or response. EMC involves the application of sound EM spectrum management:

- System, equipment, and device design configuration that ensure interference.
- Free operation.
- Clear concepts and doctrines that maximize operational effectiveness.

ELECTROMAGNETIC DECEPTION

A-9. EM deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information to an enemy or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Types of EM deception are discussed below.

Manipulative EM Deception

A-10. This type of deception involves actions to eliminate revealing or to convey misleading EM telltale indicators that may be used by hostile forces.

Simulative EM Deception

A-11. This type of deception involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.

Imitative EM Deception

A-12. This type of deception introduces EM energy into enemy systems that imitates enemy emissions.

EM Hardening

A-13. EM hardening consists of actions taken to protect personnel, facilities, and/or equipment by filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of EM energy.

EM Interference

A-14. EMI is any EM disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. It can be induced intentionally, as in some forms of EW, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like.

EM Intrusion

A-15. EM intrusion is the intentional insertion of EM energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion.

EM Jamming

A-16. EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the purpose of preventing or reducing an enemy's effective use of the EM spectrum, and with the intent of degrading or neutralizing the enemy's combat capability.

Electromagnetic Pulse

A-17. EMP is the EM radiation from a nuclear explosion caused by Compton-recoil electrons and photoelectrons from photons scattered in the materials of the nuclear device or in a surrounding medium. The resulting electric and magnetic fields may couple with electrical and electronic systems to produce damaging current and voltage surges. EMP may also be caused by nonnuclear means.

Electronic Masking

A-18. Electronic masking is the controlled radiation of EM energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy ES or SIGINT, without significantly degrading the operation of friendly systems.

Electronic Probing

A-19. Electronic probing is the intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices or systems.

Electronic Reconnaissance

A-20. Electronic reconnaissance is the detection, identification, evaluation, and location of foreign EM radiations emanating from other than nuclear detonations or radioactive sources.

Electronic Intelligence

A-21. Electronic intelligence (ELINT) is the technical and geolocational intelligence derived from foreign noncommunications EM radiations emanating from other than nuclear detonations or radioactive sources.

Electronics Security

A-22. Electronics security (ELSEC) is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications EM radiations (for example, radar).

EW Reprogramming

A-23. EW reprogramming is the deliberate alteration or modification of EW or target sensing systems or the TTP that employ them, in response to validated changes in equipment, tactics, or the EME. These changes may be the result of deliberate actions on the part of friendly, adversary, or third parties; or they may be brought about by EMI or other inadvertent phenomena. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and target sensing systems equipment. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems.

Emission Control

A-24. Emission control (EMCON) is the selective and controlled use of EM, acoustic, or other emitters to optimize C^2 capabilities while minimizing for OPSEC detection by enemy sensors; mutual interference among friendly systems; and/or execution of a military deception plan.

Spectrum Management

A-25. Spectrum management involves planning, coordination, and managing joint use of the EM spectrum through operational, engineering, and administrative procedure**s**, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

Wartime Reserve Modes

A-26. Wartime reserve modes (WARMs) are characteristics and operating procedures of sensors, communications, navigation aids (NAVAIDs), threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. WARMs are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use.

IEW Support

A-27. Electronic forms of intelligence gathering (for example, SIGINT, measurement and signature intelligence [MASINT]) comprise a significant portion of the day-to-day activities of the intelligence community. The

distinction between intelligence and ES is determined by who tasks or controls the intelligence assets, what they are tasked to provide, and for what purpose they are tasked.

A-28. ES is achieved by intelligence collection, processing, and exploitation assets tasked or controlled by an operational commander. These assets are tasked to search for, intercept, identify, locate, and report sources of intentional or unintentional radiated EM energy.

A-29. The purpose of ES tasking is immediate threat recognition and other tactical actions such as threat avoidance, targeting, and homing. ES is intended to respond to an immediate operational requirement. However, the same assets and resources, which are tasked with ES, can also collect intelligence at the same time that meets other collection requirements. Intelligence collected for ES purposes normally are also processed by the appropriate parts of the intelligence community for further exploitation after the operational commander's ES requirements are met.

Appendix B

Signal-to-Noise Ratio Reference

Signal-to-noise ratio formulas provide personnel involved in EA the tools that are necessary to compute jamming power outputs and distances. These products are necessary to fully plan and/or execute EA operations

RATIO FORMULA

B-1. The ratio formula is used to compute the maximum distance a jammer can be from a target and still be effective (Figure B-1).

$$dj = dt \sqrt[n]{\frac{Pj}{Pt\ K\left(\frac{ht}{hj}\right)^2}}$$

f	Frequency (50 MHz)
dt	Enemy transmitter location to target receiver location distance in km (9 km)
Pt	Power output of enemy transmitter in watts (5 watts)
hj	Height of jammer antenna above sear level in meters (386 meters)
Pj	Power output of the jammer in watts (1,500 watts)
ht	Height of enemy transmitting antenna above sea level (ASL) in meters (385 meters)
JSR	Jamming to signal ratio (JSR) (8:1 (9dB))
dj	Jammer location to target receiver location distance in kilometers (solve)
n	Terrain and conductivity Factor (4) 2 = Level terrain (over water, lakes, and ponds) good conductivity for a JSR of at least 2:1 3 = Rolling hills (farmland type terrain), good conductivity for a JSR of at least 4:1 4 = Moderately rough terrain (high hills), fair to good conductivity for a JSR of at least 8:1 5 = Very rough terrain (mountains or desert terrain) poor conductivity for a JSR of at least 16:1
K	Jammer tuning accuracy factor (2) 2 = For jamming FM receivers operating in the VHF range 3 = For jamming continuous wave (CW) or amplitude modulated receivers operating in the very high frequency (VHF) range

Figure B-1. Signal-to-Noise Ratio Formula

B-2. The use of this formula will provide for the creation of a range fan which, when plotted for different radios and signal strengths and broken down into varying ranges between transmitters and receivers, will allow for a

general range fan. This range fan will in turn provide the SIGINT teams with the means to effectively place teams and to determine which target areas can be affected by specific locations.

FUTURE TRENDS

B-3. The shortcoming of this formula is in its lack of any relationship to vegetation or signal frequency. These two factors affect the signal-to-noise ratio to such a degree that only a rough estimate as to a true range fan is determined. One possible solution to this problem is a system developed and designed by the Electronic Proving Ground (EPG). The Virtual Electromagnetic C4I Analysis Tool (VECAT) is designed to provide different users with powerful command, control, communications, computers, and intelligence (C4I) system analysis capabilities embedded in a user-friendly graphical user interface (GUI) environment. For example:

- A communications engineer or spectrum manager can use VECAT to plan specific communication links or perform area site analysis.
- An intelligence tester may use VECAT to plan evaluations of a sensor system immersed in a battlefield environment which would be impractical to duplicate in a field test situation.

B-4. VECAT employs terrain integrated rough earth model (TIREM) as its core EM propagation analytical engine. TIREM was developed by the Joint Spectrum Center (JSC) in the 1970s and is used for calculating EM-wave propagation loss between antennas above a point-by-point representation of the terrain elevations along an irregular profile of the earth.

B-5. TIREM evaluates the geometry of the defined path, determines appropriate modes of propagation, and applies suitable algorithms to calculate the path loss for the dominant mode. As a legacy model, TIREM suffers from lack of modern user amenities, such as GUI input interfaces and graphical output formats.

B-6. In VECAT, a powerful graphics interface is used to display the TIREM results. This allows the user to view either two- or three- dimensional (2D or 3D) data in a variety of combinations and styles. To facilitate its use, VECAT employs a Geographic Information System (GIS) and an Relational Database Management System (RDBMS) back-end. The GIS allows the user to place equipment in realistic positions. The equipment can be chosen from a database of known equipment and its deployment configuration can be stored in a database. The user can customize the calculations, thus accounting for a multitude of equipment characteristics and physical phenomena.

B-7. An important part of VECAT is the C4I standard, which is essentially the Army doctrinal dispersion of C4I assets in a geographic area of interest. With VECAT, the user can create and edit deployments and view communication links and their terrain profiles and area elevation data. VECAT provides a visual selection system, allowing the user to easily access the equipment in the deployment; the selection system permits the user to work with only those pieces of equipment satisfying specific criteria. The user can evaluate any subset of deployment. For instance, a user can

evaluate the area coverage of a specific EA asset against specific targets in the EM spectrum.

B-8. For decades, communicators have been concerned with RF propagation path loss through foliage. EPG has developed, implemented, and integrated into VECAT the EM Wave Attenuation in a Forest (EWAF) propagation model, which uses conventional inputs to estimate plausible foliage losses. The EWAF is an elementary, heuristically based foliage propagation path loss model that represents a forest as a dissipative dielectric slab lying in a more loosely half-spaced representation of the ground. Modeling the foliage by a dielectric slab provides an estimate of foliage excess-path-loss (EPL) expected in situations where meager information is available regarding wood density, conductivity, and other electrical parameters of the forest.

B-9. The EWAF model uses empirical foliage path-loss information as a basis and is therefore closely coupled to actual path-losses encountered in real-world situations. The EWAF model is not a rigorous attempt to solve the EM wave equations at the boundaries of the different representative dielectric slabs. EWAF is essentially a family of curve-fitting algorithms based on previously measured data for sparse and dense forests in the United States and Germany, as well as a very dense forest in India, where the mean annual rainfall is about 3 meters.

B-10. Features of the EWAF model include the effects of antennas within the forest, outside the forest, and above the forest; wave polarization; forest density; canopy, trunk, and undergrowth losses; antenna beamwidth; wet foliage; lush foliage; and other physical or forest conditions. The model provides a good estimator for EPL due to foliage anywhere in the world.

B-11. VECAT provides a powerful, flexible C^4I analysis tool for a wide range of users. The interface is user-friendly and provides output customized to the user's needs. VECAT is expandable and well documented. It is developed to contemporary standards and uses and reuses existing software when practical. VECAT is a modern system, available now to meet a wide variety of user's needs. VECAT will provide an easy medium in which to perform engineering analyses, evaluations, and planning studies in the following functional areas:

- Fundamental EM wave propagation analyses over digital terrain.
- Receive signal level (RSL), often incorporating 3D antenna patterns.
- LOS and terrain masking effects.
- Path profile terrain evaluations.
- Signal-to-interference ratio (S/1) and bit error rate (BER) studies.
- Electromagnetic environmental effects (E3) electric field distributions.
- Spectrum usage and signal modulation.
- Co-site EMI, remote interferer, and jammer studies.
- Fade-and-noise modeling.
- EM wave propagation through foliage.

Appendix C

Electronic Deception

Electronic Deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronic dependent weapons. Electronic deception is both parts of EW and military deceptions. Normally, an electronic deception is conducted as part of a larger deception, and are seldom conducted alone. Division is the lowest level at which a deception plan can be initiated, and the commander must approve all deception plans. Historically, deception operations originate from EAC.

TYPES OF ELECTRONIC DECEPTION

C-1. Among the types of electronic deception are—

- **Manipulative Electronic Deception (MED).** Actions to eliminate, reveal, or convey misleading, telltale indicators that may be used by hostile forces.
- **Simulative Electronic Deception (SED).** Actions to represent friendly, notional, or actual capabilities to mislead hostile forces.
- **Imitative Electronic Deception (IED)**. The introduction of EM energy into enemy systems that imitates enemy emissions.

C-2. Although electronic deception is usually thought of in terms of communications, electronic deception is also conducted using digital (analog) emissions. The signals could mimic the data flows issuing from a TOC when in reality it is a jammer putting out a signal pre-recorded for this mission.

MANIPULATIVE ELECTRONIC DECEPTION

C-3. MED uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit is going to attack when it is actually going to withdraw, the unit might transmit false FS plans and requests for ammunition.

C-4. MED is used to cause the enemy to splinter his intelligence and EW efforts to the point that they lose effectiveness. It is used to cause the enemy to misdirect his EA and ES assets and therefore cause fewer problems with friendly communications. Used in these ways, MED is an EP technique.

SIMULATIVE ELECTRONIC DECEPTION

C-5. SED uses communication and noncommunication signals to mislead hostile forces as to friendly units and/or the capabilities of friendly units. There are three types of SEDs:

- **Unit Simulation.** The use of actual equipment or specially designed simulators to indicate that a unit is in a certain location during a specified period.
- **System Simulation.** The use of systems that give off emissions peculiar to a particular organization. A countermortar or counterbattery radar is peculiar to an artillery unit; therefore, by turning on that type of radar you can indicate the probable location of an artillery unit.
- **Activity Simulation.** The operation of noncommunication emitters to imply a type or change of activity by a unit. For example, placing surveillance radars in a typical defensive array when, in fact, the intention is an attack.

IMITATIVE ELECTRONIC DECEPTION

C-6. In IED, the enemy's EM emissions are imitated to mislead the enemy. Examples include entering the enemy communication nets by using his callsigns and radio procedures, and then giving enemy commanders instructions to initiate actions which are to our advantage. Targets for IED include any enemy receiver and range from cryptographic systems to very simple, plain-language tactical nets. IED can cause a unit to be in the wrong place at the right time, to place ordnance on the wrong target, or to delay attack plans. Imitative deception efforts are intended to cause decisions based on false information that appears to the enemy to have come from his own side.

C-7. Properly used, IED can be decisive on the battlefield. However, to be effective, IED requires electronic equipment capable of convincingly duplicating the functions of enemy equipment. IED is done if—

- (The transmitter) is compatible with the intended receiver station equipment.
- (The transmitter) has sufficient power to transmit to the receiver station.
- A proficient linguist (if voice transmissions are used).
- An operator capable of imitating the transmitting style of the enemy manual Morse operator (if continuous wave is used).

C-8. If available, however, captured enemy equipment (CEE) should be used to ensure that the technical characteristics of signals are authentic.

ELECTRONIC DECEPTION PLANNING

C-9. Electronic deception planning determines how to use EM equipment to mislead the enemy and cause him to do something to our advantage. Each

piece of electronic and associated equipment has its own electronic signature. These signatures are exploited in deception.

C-10. The G3 usually plans and supervises deceptions. The EWO is usually responsible to the G3 for the electronic deception plan. All of these personnel work with the G2 to determine the electronic activities most likely to be intercepted by enemy SIGINT.

C-11. Careful integration of electronic deception with visual, sonic, and olfactory actions is critical. What the enemy detects electronically must remain consistent with other sources of intelligence reports. Because of the reliance placed on EM radiation (for example, communication, surveillance, navigation) this aspect of deception requires close attention. Although electronic deception can be the sole act of deception, the effect is often of short duration.

C-12. The enemy's success depends upon his knowledge of your emitters. Success in MED and SED depends on understanding how your emitters appear to the enemy. The SIGINT team should keep a profile (database) of a command's voice and digital (analog) emitters. This is to determine how best to electronically portray a desired portion of that command. When planning MED and SED, it is usually necessary to consider all the command's EM emitters. It is necessary to consider what is occurring and what should occur with all EM emitters in the unit's area.

C-13. Similarly, when planning an electronic deception, consider all unit electronic activities, such as—

- Actions that support the current operation as well as those that will support the deception operation.
- All actions which must be integrated and deconflicted to prevent one activity interfering with another.

C-14. Some considerations for planning are—

- Close control and coordination will be necessary, especially during MED.
- The staff plans to avoid confusing friendly operators with deception communications or with unique returns on digital (analog) equipment.

C-15. Time is critical. Given sufficient time, the enemy can discover even the most complex electronic deception. A deception intended to deceive the enemy for two or three days must include a well-coordinated electronic deception that covers all electronic emitters.

- Adequate for a deception for only a short period just before an attack.
- The electronic deception plan can be relatively simple.
- Enemy capabilities are critical. If the enemy cannot detect your electronic emitters, the electronic deception will fail.

C-16. The commander can perform MED and SED as long as he uses only equipment under his control. IED can only be done with permission of the appropriate commander—within a division, this is usually the division commander. This restriction is to ensure that IED does not jeopardize the SIGINT effort. IED, if recognized by the enemy, will provide data concerning

the friendly ES effort. This could cause the enemy to improve his communications security (COMSEC) and procedures to reduce the effectiveness of the friendly SIGINT efforts. Coordination with higher will always occur before any MED or SED operations begin.

C-17. False emanations must be—

- On signals strong enough to reach the enemy.
- On a frequency the enemy can intercept.
- In a modulation the enemy can intercept.

ELECTRONIC DECEPTION TECHNIQUES

C-18. The following are electronic deception techniques:

- Leave a significant sample of regimental or battalion headquarters communication in place while the headquarters moves to another location.
- Broadcast false information with the intention of having the enemy receive the message and commit his forces into an area of our choosing.
- Broadcast false unit strengths, dispositions, or locations to confuse the enemy.
- Exchange operators among units or overload one unit with operators whose characteristics are probably known to the enemy.
- Place multichannel communications in a battalion area to show a larger force.
- Pad traffic on secure links to deceptively show a buildup for an attack. This technique applies to both voice and message traffic when encrypted.
- Use callsigns and frequencies to lead the enemy to incorrect net structures.

ST 2-22.7 (FM 34-7-1)

TACTICAL HUMAN INTELLIGENCE AND COUNTERINTELLIGENCE OPERATIONS

US Army Intelligence Center and Fort Huachuca
Fort Huachuca, Arizona 85613-6000

APRIL 2002

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

- **Tactical HUMINT Support to Force Protection** - A commander's force protection program encompasses many assets designed to provide survivability to the force. HUMINT collection can supply information in support of a supported commander's force protection program while CI can use its unique collection capabilities to identify FISS and terrorist threats. Support to force protection can and should be applied to all aspects of a unit's operations.

CI INVESTIGATION AND TECHNICAL SUPPORT

4-7. CI investigations are operations requiring CI certification. Only CI agents with a badge and credentials may conduct these types of operations. Due to their credentials, there are often legal restrictions regarding the use of CI agents that do not apply to HUMINT collectors. For example, the use of CI agents to collect information on criminal activities is severely curtailed. HUMINT collectors, on the other hand, are prohibited to engage in CI investigative operations in any capacity other than as a translator or assistant.

- **CI Investigations** - CI agents are trained to conduct investigations into national security crimes. The average tactical HUMINT team will not spend a great amount of time conducting CI investigations and will require assistance from operational and strategic CI assets to conduct any more than initial CI investigations. Areas of CI investigation include espionage, terrorism, treason, subversion, sedition, and intrusion of automated information systems. Although HUMINT and CI personnel are capable of conducting a wide range of each other's duties, only CI personnel are authorized to conduct CI investigations. Investigations are conducted in accordance with ARs 381-10, 381-12, and 381-20.
- **CI Technical Support** - CI elements from INSCOM bring some valuable technical capabilities to a contingency area. These include TSCM capabilities, TEMPEST and C^2 protect, and polygraph support.

Human Sources

4-8. Every person—friendly, hostile, or neutral—is a potential source of information. The HUMINT information collection system uses various methods to collect information from a number of sources. The tactical HUMINT team does not confine itself to one method of collection or a single type of source. The effectiveness of HUMINT collection lies in creating a balanced mix of collection methods applied to a variety of sources. Three levels are used to distinguish between the types of contacts:

- Level 1 – One-time contact.
- Level 2 – Continuous contact.
- Level 3 – Formal contact.

4-9. The following sources are not all-inclusive nor are the listed categories exclusive. For example, a local national employee might be a walk-in source and later be developed as a CFSO source. With the exception of Level 1, there is no limit on the number of times a team

can meet sources without making them Level 3. However, all sources must be registered with the J/G2X after the first meeting.

LEVEL 1 - ONE-TIME CONTACT

4-10. The one-time contact is a source of information of value who was and will be encountered only once. A one-time contact could, for example, be a traveler who happened to pass through the AO. Other than the information obtained from a one-time contact, the tactical HUMINT team must make a reasonable effort to obtain as much basic data as possible about the one-time contact. Complete name, occupation, address, and other basic data of this source are crucial for a thorough analysis of the information provided.

4-11. The one-time contact and the information he provides cannot be assessed and evaluated independently; however, the information provided by a one-time contact must be reported and corroborated through other HUMINT sources and even other intelligence disciplines. If a one-time contact is encountered for a second time and provides information of value, then they may be treated as a developmental lead.

Walk-In

4-12. The walk-in is any person, regardless of affiliation, who volunteers information of value to US forces on his own initiative. The walk-in source may volunteer information by approaching a tactical HUMINT team, other R&S elements, or US forces in general anywhere in the battlespace.

4-13. The supported unit must have in place a program to identify, safeguard, and direct the walk-in to the appropriate collection asset for an interview. The collection asset will interview the walk-in to determine the type of information the source has and to determine and evaluate the reliability of the individual.

4-14. After identifying the type of information, the collector determines if he has the jurisdiction to collect that information. If, for example, the walk-in wishes to report a crime, the collector refers that individual to the proper agency. Systematic questioning plans, deception, detection techniques, and cross-checking of information are used extensively in the evaluation process. Concurrently, there are national level directives, DOD directives, and Army regulations that direct specific actions to be taken with a walk-in.

4-15. When dealing with a walk-in source, the supported unit and the collection asset must guard against adversary intelligence or other intelligence collection attempts; they must also protect legitimate sources of information. The walk-in is thoroughly debriefed on all areas of information relevant to collection requirements, and any information of value is reported.

Development Lead

4-16. A developmental lead is an individual identified through social and professional status, leads, source profiling, or other techniques that has knowledge required by the commander. As such, the tactical HUMINT team normally should express operational interest as soon as possible. While not every developmental lead becomes a source of information, the tactical

HUMINT team should see each developmental lead as a potential source of information and apply the appropriate security measures.

4-17. The developmental lead is continuously assessed to verify his placement and access to the type of information the tactical HUMINT team is seeking. Additionally, the tactical

HUMINT team continuously assesses the motivation and characteristics of the developmental lead.

LEVEL 2 - continuous contacts

4-18. These are individuals met by HUMINT and CI personnel for the purposes of collecting information in response to the commander's PIR.

Local National and Third-Country National Employees

4-19. Local national and third-country national employees are non-US personnel from either the country in which the US forces are operating or a third country who are either employed by US forces directly or through a contractor to provide logistical support and services. One of the purposes of locally employed personnel screening is to assess these individuals as potential sources of information.

4-20. Local national and third-country national employees can be a prolific source of information about local attitudes and events, particularly in a restrictive environment where US contact with the local population is curtailed. Their information can be significant in a force protection role. The collector must register these individuals with the J/G2X.

4-21. All locally employed personnel are considered a security risk and must be screened and evaluated by the collector. There are situations when locally employed personnel approach US forces to volunteer information. In these situations, they must be dealt with as walk-ins.

Displaced Personnel

4-22. Displaced personnel include refugees and émigrés. They are an excellent source of information about denied areas and can be used to help identify threat agents and infiltrators. The degree of access HUMINT collectors have to displaced persons depends on the rules of engagement (ROE) and Status of Forces Agreements (SOFAs) in effect. HUMINT collectors can work with CA or other programs dealing with displaced persons.

4-23. Displaced persons are normally considered one-time sources but may be incorporated into other long-term collection programs if their degree of knowledge warrants this. In this case adherence to the restrictions involving source operations is necessary.

US Forces

4-24. US forces have many opportunities to interact with the local population in the normal course of their duties in operations from PMEs to MTW. They are perhaps the most under-utilized HUMINT collection resource. Some US forces, such as combat and R&S patrols, are tasked and debriefed by the appropriate level S2, but others, such as medical teams or

engineers who have extensive contact with the local population, are seldom debriefed. Commanders and staff members who serve as liaison with the local population and local government officials can be fruitful sources of information. CA, PSYOP, MP, and other elements also have legitimate reasons to conduct liaison and should be debriefed as appropriate.

4-25. The friendly force debriefing effort can succeed only with command emphasis. HUMINT collection elements need to coordinate with local units to identify those individuals who would be most profitable to debrief and to further coordinate with them for time to conduct the debriefing. HUMINT collectors must ensure that their friendly force debriefing effort does not interfere with the normal duties of the person being debriefed. Except for patrols and R&S elements whose job is information collection, US forces should not be tasked to collect specific information but should be questioned only on what they encountered in the normal performance of their duties.

Official Liaison

4-26. Liaison with local military, government, or civilian agency officials provides an opportunity to collect information required by the commander. The tactical HUMINT team meets with these officials to conduct liaison, coordinate certain operations, collect information, and obtain leads to potential sources of information.

4-27. Elicitation is the primary technique used with liaison contacts, although in many cases there is a more formal exchange of information. Information obtained by these elements through liaison normally tends to be the party line and may not be entirely accurate or complete.

Detainees

4-28. A detainee is any person captured or otherwise detained by an armed force. An EPW is a detainee who meets the criteria of Articles 4 and 5 of the Geneva Convention relative to the treatment of prisoners of war.

4-29. Within the limits of the ROE and SOFAs, detained persons may be interrogated. They are frequently excellent sources of information but in many instances the access of the HUMINT collector to the detainees is severely curtailed. For example, when supporting a counterinsurgency, the supported government may consider all captured insurgents to be criminals and not allow US forces access to them. In these instances, US HUMINT collectors should attempt to sit in during local questioning; they could submit questions or, at a minimum, coordinate to receive the reports from the local authority. The US HUMINT collector must remember that, regardless of the legal position of the detainee, they must be treated in accordance with the appropriate Geneva Convention.

LEVEL 3 - FORMAL CONTACT

4-30. These are individuals who have agreed to meet and cooperate with HUMINT and CI soldiers for the purpose of providing information. HUMINT and CI soldiers use Level 3 contacts

to provide specific information. While these meetings are overt, Level 3 contacts are met discretely to protect their relationship with HUMINT and CI soldiers. Knowledge of their meeting with HUMINT and CI soldiers is restricted. Tactical HUMINT teams take extraordinary measures to protect their relationship with the contacts.

OTHER SOURCES

4-31. OTHER SOURCES ARE ANY SOURCES NOT DISCUSSED ABOVE. GENERALLY, THEY FALL IN TWO CATEGORIES: OPEN-SOURCE INFORMATION AND CAPTURED ENEMY DOCUMENTS (CEDS) OR CAPTURED ENEMY EQUIPMENT (CEE).

OPEN-SOURCE INFORMATION

4-32. Open-source information is publicly available information appearing in print or electronic form. Open-source information may be transmitted through radio, television, newspapers, commercial databases, electronic mail networks, or other electronic media like CD-ROMs. Whatever form they take, open sources are —

- Not classified at their origin.
- Not subject to proprietary constraints.
- Not the product of sensitive contacts with US or foreign persons.

4-33. In all operations, open-source collection is a valuable addition to the overall intelligence collection effort. Open-source information supplements the HUMINT collection effort, and all types of open sources must be considered for exploitation. Open sources are evaluated and categorized as friendly, neutral, or hostile. HUMINT collectors—due to their knowledge of the area, language capability, and DOCEX training—are excellent exploiters of open- source information produced by and about foreign adversaries.

4-34. Certain high value open-source information sources may be identified for continuous monitoring. Other open-source information sources may be identified to screen for the presence or lack of specific indicators. In addition, the information obtained from open sources is extremely helpful for the tactical HUMINT team members to be current with the latest developments in the AO, which enables them to establish rapport and effectively converse with their sources.

CAPTURED ENEMY DOCUMENTS OR CAPTURED ENEMY EQUIPMENT

4-35. A CED is any piece of recorded information obtained from the threat or a hostile party, which subsequently comes into the hands of the US forces. In certain operations from PMEs to

MTW, such as counterinsurgency, CEDs may be a more valuable source of information than human sources. (See FM 2-22.3 (FM 34-52) for more information on the DOCEX process.)

4-36. CEE is any piece of equipment obtained from a threat, which subsequently comes into the hands of US forces. CEE ranges from the smallest specialized electronic devices to huge pieces of machinery and weapons or weapons systems. While not specifically a HUMINT task, HUMINT collectors, because of their training in human information collection and DOCEX, frequently become involved in equipment exploitation. HUMINT collectors support CEE exploitation by questioning equipment operators or translating operational manuals and writings about the equipment (such as data plates, warnings, and other instructions).

Chapter 5

Team Operations

The tactical HUMINT team is the basic unit of a robust architecture which extends from the foxhole to the departmental level. The team, which is your eyes and ears, is trained and equipped to plan, collect, investigate, and analyze threat information to support the MDMP and force protection effort.

Tactical HUMINT teams are capable of conducting a variety of activities. These units are highly modular and mobile. They require state-of-the-art automation and dedicated and secure communication equipment to report and disseminate time-sensitive information to commanders as well as to higher, lower, and adjacent units. Configured in response to a commander's needs, tactical HUMINT teams are tactically tailored based on the type and phase of a military operation. Specifically, they can—

- Collect information from human sources to answer the commander's PIR and IR.
- Receive and input threat database information.
- Manipulate and analyze information.
- Incorporate information into their operational planning.
- Produce tactical intelligence information reports and products.

MI unit commanders must ensure their tactical HUMINT teams have the necessary equipment to accomplish the mission. They provide operational support as needed to teams that are DS to another unit. FM 2-22.3 (FM 34-52), FM 2-01.2 (FM 34-60), and various echelon MI field manuals provide more information on HUMINT and CI support to an MTW.

CONCENTRIC RINGS OPERATION METHODOLOGY

5-1. Most operations are initiated with the establishment of a lodgment and defense of that lodgment area. There is a subsequent expansion of operations to encompass the entire AO.

FM 34-2-1

TACTICS, TECHNIQUES, AND PROCEDURES FOR

RECONNAISSANCE AND SURVEILLANCE AND INTELLIGENCE SUPPORT TO COUNTERRECONNAISSANCE

HEADQUARTERS,
DEPARTMENT OF THE ARMY

DESTRUCTION NOTICE—Approved for public release; distribution is unlimited.

There is an interrelationship between all aspects of the intelligence cycle. Your collection plan has a direct effect on how you--

o Process information and disseminate intelligence during the present battle.

o Direct your intelligence efforts for future battles.

The R&S plan marries the IPB with assets available for information collection. It organizes and prioritizes information requirements. This results in R&S taskings to units through the S3.

RECONNAISSANCE AND SURVEILLANCE PRINCIPLES

Now that we have defined the terms, let us discuss the two principles of R&S. They are--

o Tell commanders what they need to know in time for them to act.

o Do as much as possible ahead of time.

TELL COMMANDERS WHAT THEY NEED TO KNOW IN TIME FOR THEM TO ACT

This principle is of paramount importance. You must develop the R&S plan so that it directly addresses what the commander wants to know. In essence, the R&S effort (as with the intelligence effort in general) is commander-oriented and commander-directed. Therefore, you cannot develop a successful R&S plan until you know exactly what the commander needs to know.

The commander's questions which positively must be answered in order to accomplish the mission are PIR. They are the start point for the R&S plan. The clearer and more precise the commander's PIR, the better you will be able to develop the R&S plan to answer them.

How do PIR come about? As part of the mission analysis process, you and your commander study the mission given to you by higher headquarters. You develop specified, implied, and essential tasks. As you do this, you should also be able to identify gaps in your understanding of the battlefield situation.

The following are examples of possible gaps:

o Which avenue of approach (AA) will the enemy use, and when?

o Which fixed- and rotary-wing air AAs will the enemy use?

o How will the enemy deploy in their attack?

o Where will the enemy commit their second echelon forces?

o What are the enemy reconnaissance forces, tactics, and capabilities?

o Where is the enemy main supply route (MSR)?

o Under what circumstances will the enemy use NBC weapons? How will they be employed?

o What are the enemy subsequent and fallback positions, and routes from their main defensive positions to the fallback positions?

o In what strength will the enemy counterattack, and where are the armor counterattack forces?

o Where are the enemy observation posts (OPs) and listening posts (LPs)?

o Where are the enemy antitank (AT) helicopters?

o Where are the enemy TOCs and tactical command posts, relays, and communications sites?

o Where are the enemy logistic and support areas?

o What effects of weather provide a key advantage or disadvantage to you or the enemy?

o Where are the enemy obstacles and fire sacks?

o Where are the enemy main defensive positions?

o Where and when will the enemy counterattack, and how will they counterattack?

o Where are the enemy AT weapons?

o Where is the enemy artillery?

Essentially, you and your commander try to zero in on exactly what will determine the outcome of the battle. Many times, the commander will tell you what is of the most concern. It is the responsibility of the commander to state PIR. However, the S2 and the S3 can assist in this process by presenting their own analyses of the mission.

Remember, PIR drive your R&S efforts; so it is critical that you understand just exactly what your commander needs to know in order to fight.

Try to keep the commander's PIR as specific as possible. The more general the question, the harder it is to answer. Instead of asking, “With what force will the 34th Motorized Rifle Regiment attack?", try to discern exactly what it is your commander is looking for. If the commander wants to know how the 34th will initially deploy, it is better to ask, "Will the 34th attack in column, with two battalions leading, or with three battalions on line?"

Similarly, is the commander concerned with finding the

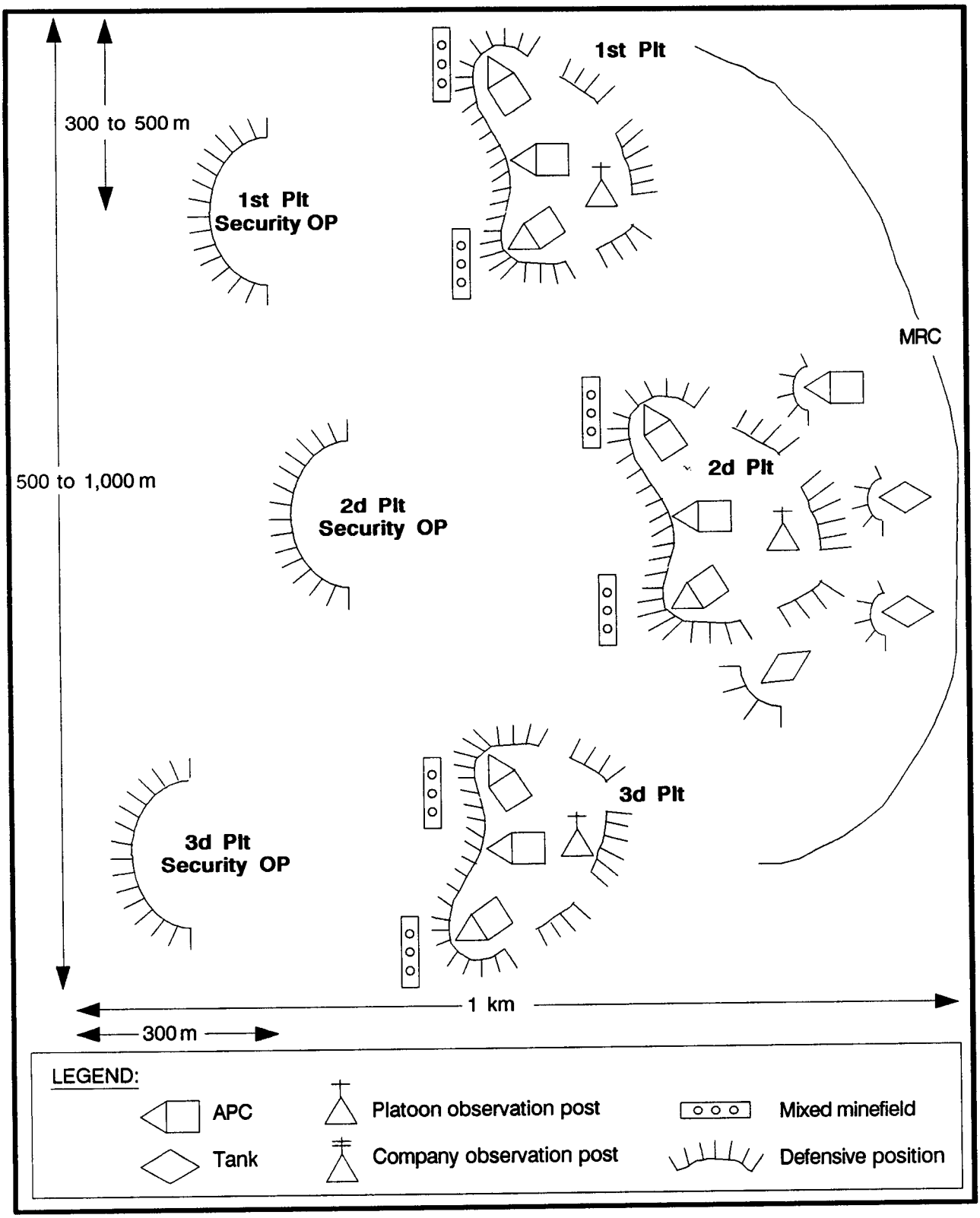


Figure 2-8. Doctrinal template of an MRC (reinforced) strong point.

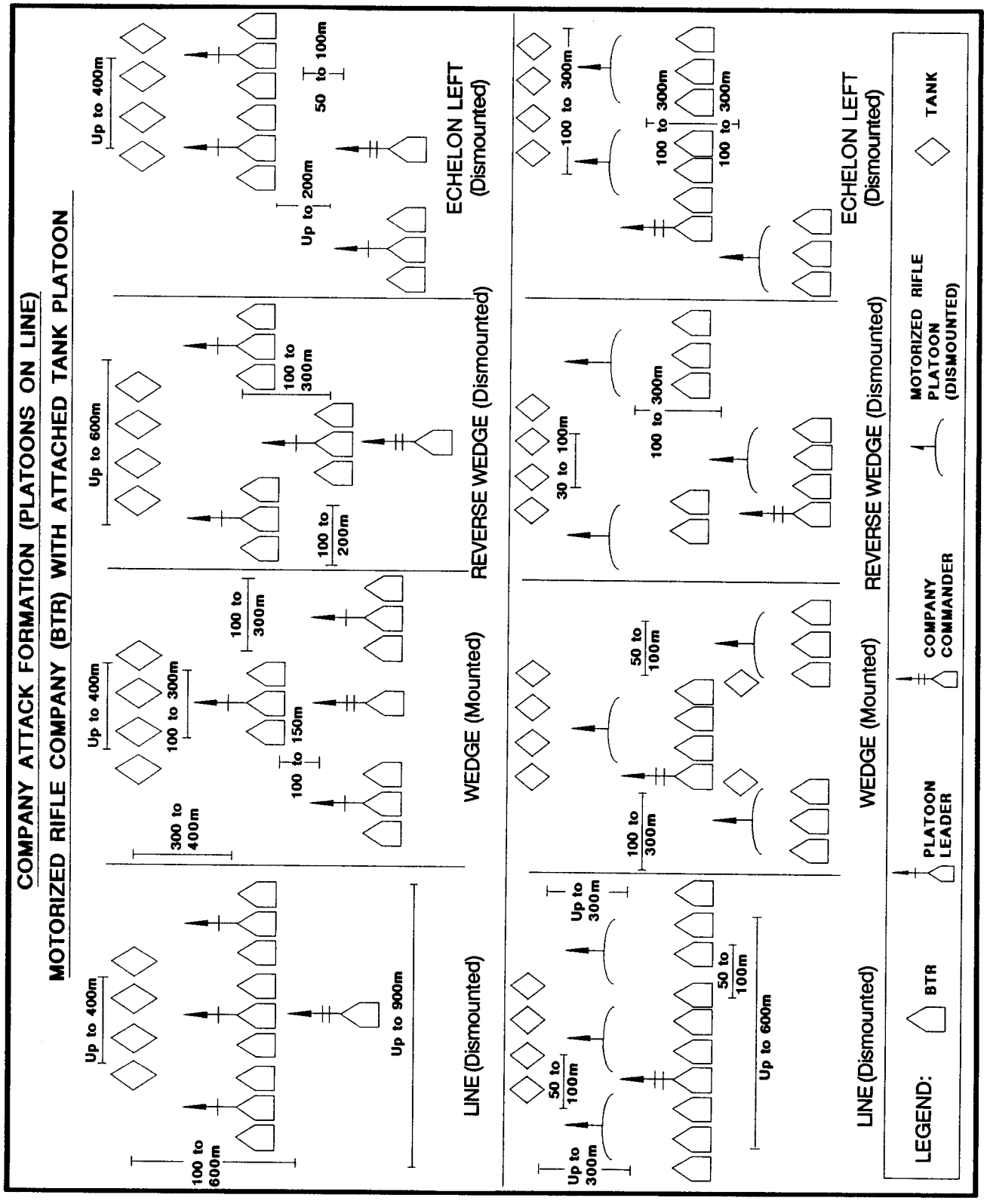


Figure 2-9. Offensive doctrinal template.

o Report trafficability along AA.

o Establish OPs overlooking AA.

o Reconnoiter terrain and suspected enemy locations capable of overmatching and placing effective fire on the AA.

o Detect locations and strength of enemy R&S assets along the AA.

RECONNAISSANCE OF THE OBJECTIVE

Typical reconnaissance missions in the area of the objective are--

o Pinpoint fighting positions. Provide strength, weapon orientations, and description of fighting positions.

o Detect obstacles and prepare to mark. Detect breaches, gaps, and bypasses.

o Reconnoiter area around the objective (area depends on METT-T) to detect possible reinforcements or counterattack elements.

o Establish OPs to maintain surveillance of the objective.

As reconnaissance assets conduct these missions, you must ensure security, surveillance, and CR assets are providing coverage to the maneuver elements while they are preparing for this offensive operation. It appears to be two distinct R&S missions taking place at the same time. The first mission is providing support to the units that are preparing for the offensive OPORD. The second mission conducts R&S to answer PIR concerning the actual offensive operation.

SURVEILLANCE OF THE OBJECTIVE

Now it is time to focus on the second area of planning consideration which stresses surveillance. Surveillance focuses on--

o The objective.

o Terrain along the friendly avenue of approach (AA).

o Possible enemy reinforcement routes.

During this phase, you must make sure the S3 and all maneuver elements know the locations of surveillance assets.

Surveillance of the objective should detect any changes while the friendly elements are maneuvering forward. The surveillance assets report any enemy leaving or entering the objective area.

Any terrain that can control the friendly AA should be covered with surveillance or controlled by one of the seven BOS listed at the bottom of the DST.

Any routes leading into the friendly AA or the objective should be covered with surveillance to provide early warning of an enemy counterattack or reinforcements approaching. Again, these surveillance operations occur while the friendly elements are maneuvering toward the objective.

ONGOING RECONNAISSANCE AND SURVEILLANCE PLANNING

The third area of planning consideration focuses on both R&S missions. This area concerns planning R&S missions once your unit takes the objective. The S3 can now task subsequent R&S missions to those assets which provided surveillance to the maneuver elements. These R&S missions depend on the type of follow-on missions planned.

If the unit's mission is to reconsolidate and prepare to continue the attack to a subsequent objective, you should have a plan to continue R&S activities forward to the next objective. Remember, planning is continuous. After you accomplish this, your unit can implement missions discussed in supporting the second and third areas of planning considerations. A key scout mission is maintaining visual contact with the enemy.

If the unit's mission is to occupy and defend the objective, you should recommend an R&S plan stressing early warning and CR operations.

If the unit's mission is to pursue the fleeing enemy, you could recommend that scout elements provide flank security as other maneuver elements conduct guard operations.

The most important aspect of the final planning consideration is that it be planned out well in advance. This ensures the assets are prepared to execute the mission, not reorganizing the objective.

The three areas of planning considerations previously stated work particularly well in a deliberate attack. You can apply these same principles for a movement to contact.

Do not be misled into thinking these three areas of planning considerations take place independent of each other at different times. On the contrary, many times these missions overlap.

We have shown you a technique for constructing complete R&S plans in offensive operations. Refer to Chapter 12 for examples.

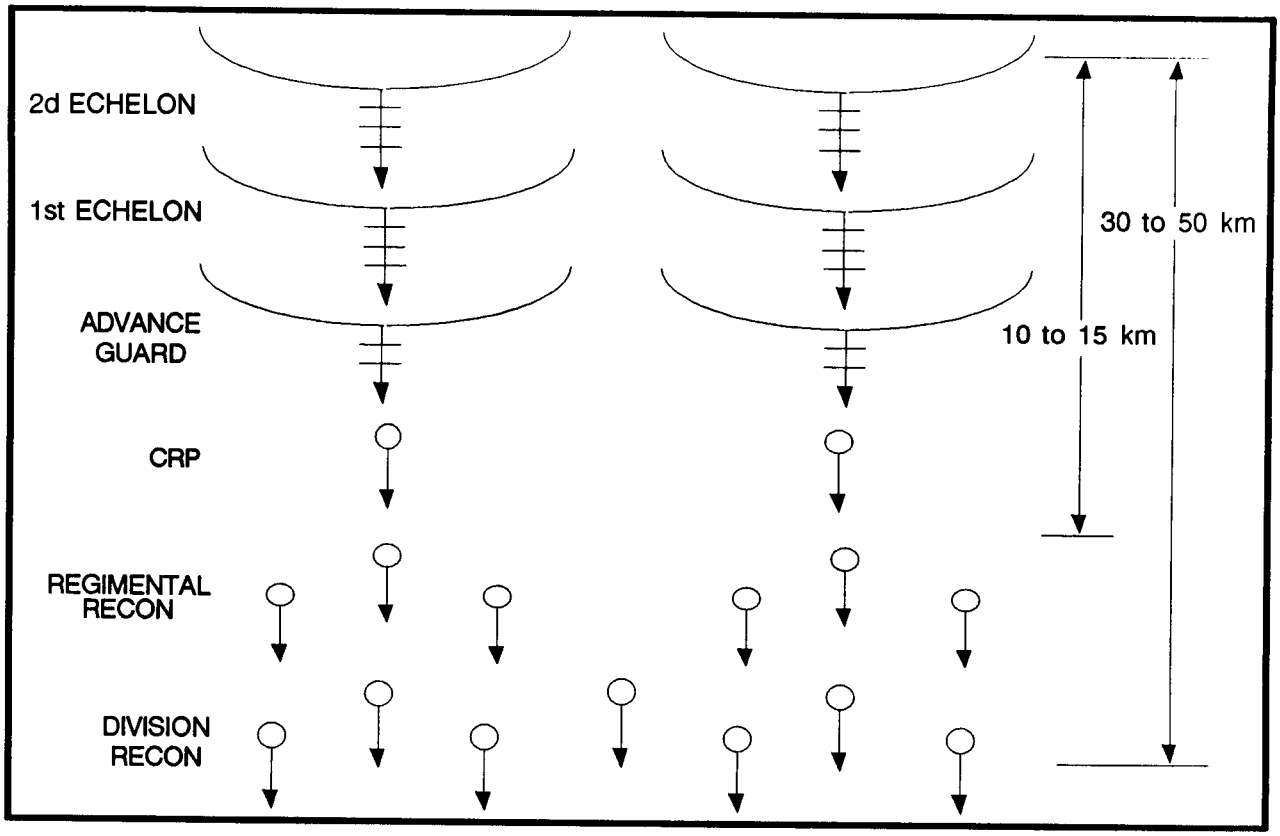


Figure 10-3. Soviet doctrinal deployment (meeting engagement).

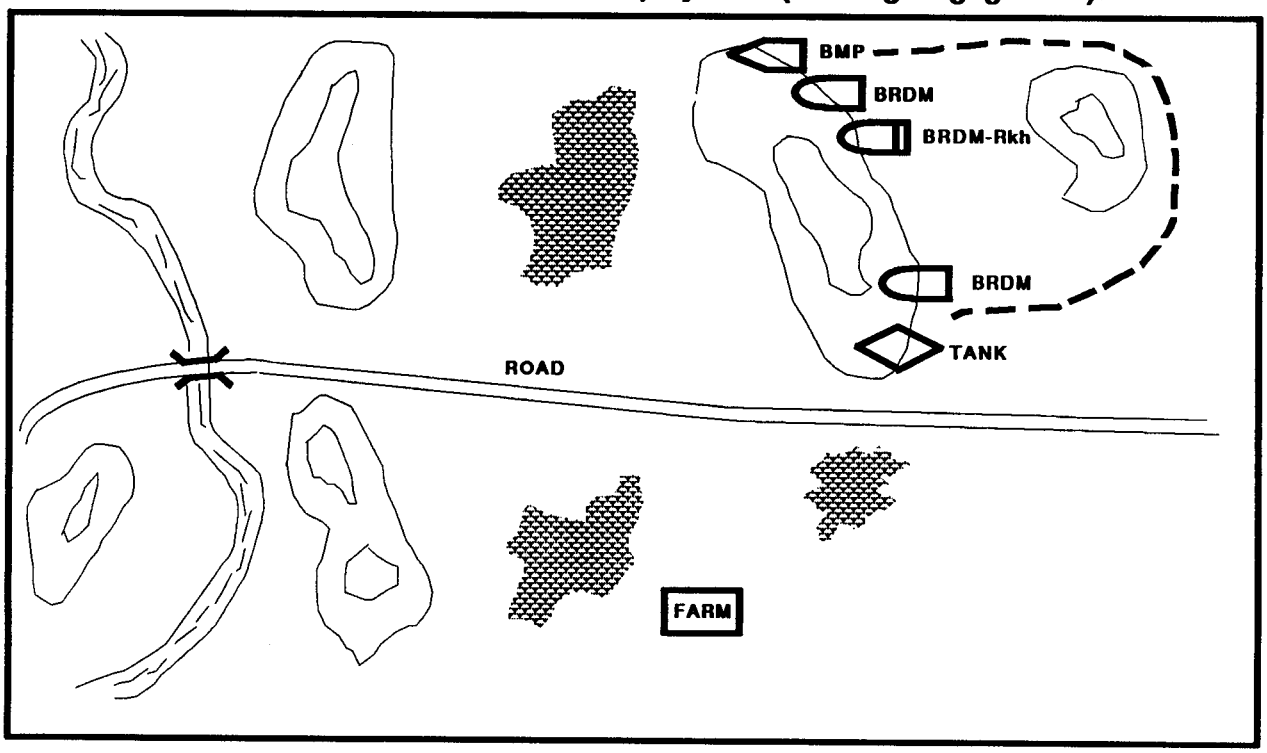


Figure 10-4. Soviet reconnaissance overwatch.

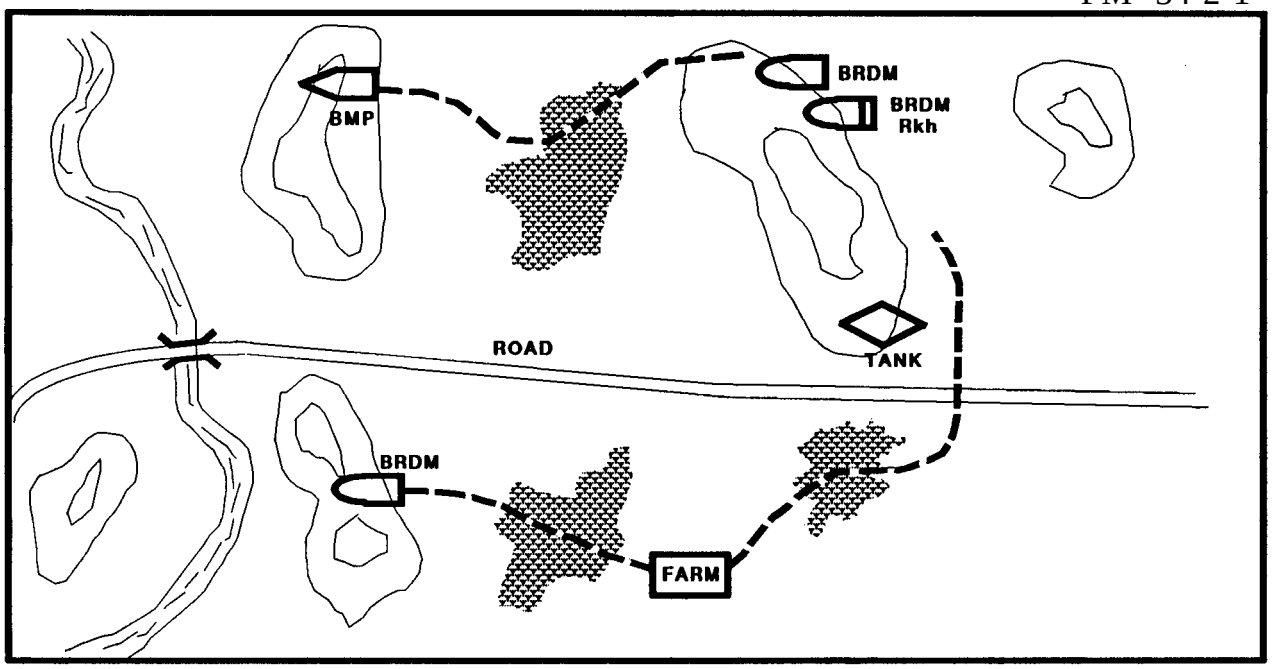


Figure 10-5. Soviet reconnaissance overwatch with patrols.

situation templates which depict enemy reconnaissance movement. Such templates allow you to develop your event template; and let your S3 visualize how you expect the enemy to conduct their reconnaissance battle. Figure 10-6 is a sample of one such situation template.

SITUATION TEMPLATE

Do not make the mistake of thinking the enemy's reconnaissance will use the same AAs as the enemy main force. Remember, enemy reconnaissance elements will most likely operate as two or three vehicles. Such small elements can traverse almost any kind of terrain. Keep in mind, the mission of reconnaissance is to seek and report information, not to fight. Therefore, enemy reconnaissance will use routes that have plenty of concealment and cover.

Also remember, enemy reconnaissance is looking for the best route of attack; the enemy may decide that attacking over rough terrain is preferable to attacking open, but heavily defended, country. For this reason, be sure to consider your entire AI when you develop your situation templates. Do not get "tunnel vision" and consider only obvious AAs or MCs.

Look at all ways the enemy can enter your sector, including using No-Go terrain! As a general rule, the more concealment or protection a route provides, the more likely it will be used by reconnaissance elements. The outcome of well prepared

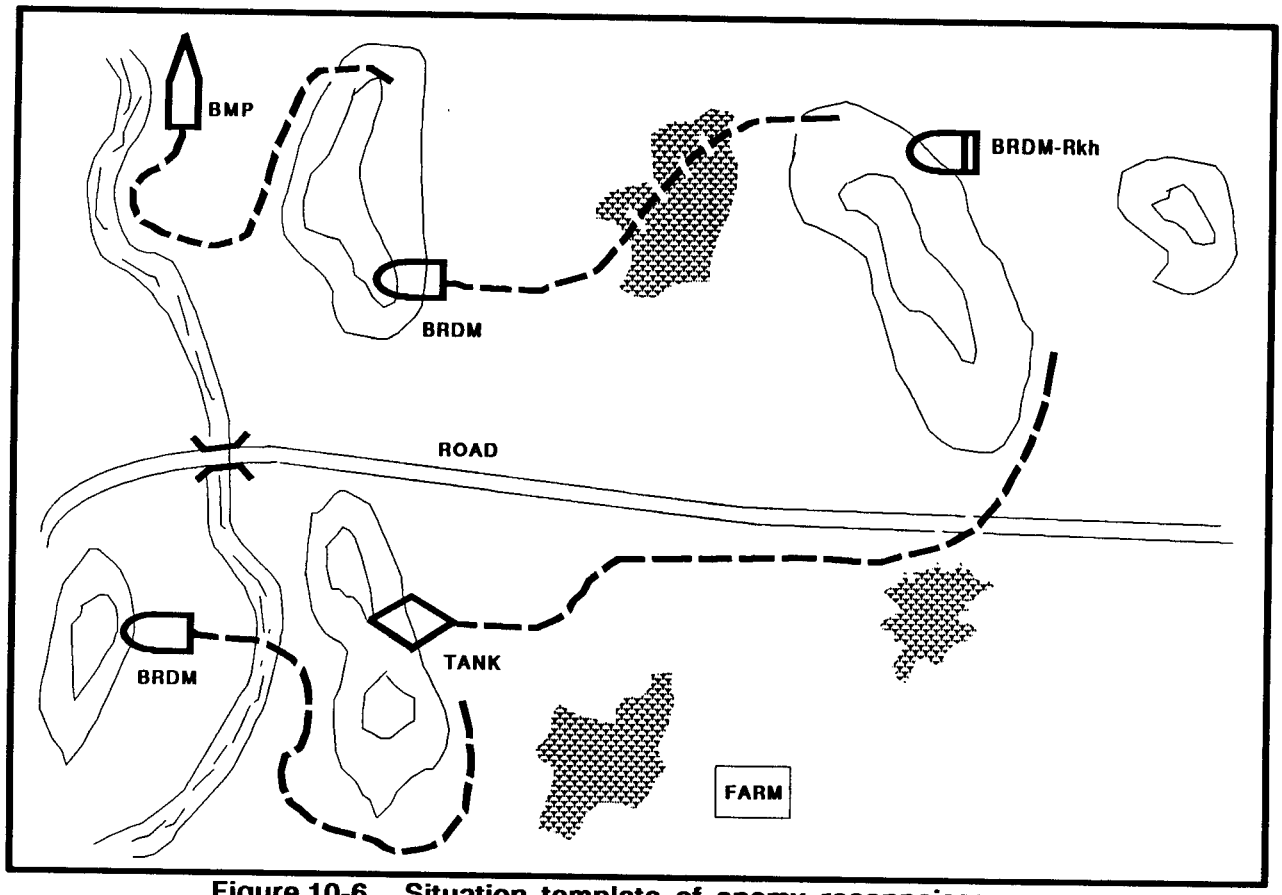


Figure 10-6. Situation template of enemy reconnaissance.

situation templates is a commander and staff that have a good indication of what the enemy will look like on the battlefield. This eventually will save your R&S assets many hours of unnecessary reconnaissance or surveillance.

EVENT TEMPLATE

Based on your situation templates, develop your event template. Your event template will show where on the battlefield you expect to see enemy reconnaissance elements. Then concentrate your R&S attention on those areas (NAI) to detect enemy reconnaissance activity.

Remember, the key to CR intelligence support is finding those enemy reconnaissance units before they can discover friendly positions and report back. Therefore, you must carefully study the effects of weather and terrain on enemy

CHAPTER 11

RECONNAISSANCE AND SURVEILLANCE IN LOW-INTENSITY CONFLICT

During LIC operations, R&S must provide your commander a wide range of information in a complex environment.

FACTORS

Factors to consider when planning R&S in an LIC environment include--

o US forces mission--counterinsurgency, combatting terrorism, peacekeeping operation, or peacetime contingency operations.

o Threat--conventional forces, insurgent forces, terrorists, demonstrators, or a combination of two or more.

o Environment--social, psychological, political, and economic factors. Terrain and weather are also important considerations.

o Host nation government--support, information sharing, security forces, and military forces.

The US force's mission, environment, and host-nation government are influences that have an affect on what we do offensively or defensively. However, the LIC threat will require you to spend the most time learning how to predict the enemy's next move.

THREAT

The LIC threat can range from demonstrations, terrorist acts, insurgent or guerrilla activity to confrontations with conventional forces. The characteristics of a threat force depend on the level of insurgency. US maneuver forces will most likely face insurgent forces or a hostile country conventional military force. Your unit may face demonstrators or terrorist threats. But primary population control responsibility is with the host nation.

Insurgent or guerrilla forces usually fight in small cells. They carry light weapons and can concentrate forces against major facilities, then disperse after the operation. Insurgent forces can operate in urban areas but prefer remote areas for better concealment and security. You can expect to fight squad- to platoon-size forces when facing insurgent forces. They will rely on--

o Well-planned ambushes.

o Attacks on soft targets.

o Sniper and mortar attacks.

The objective is to demoralize and frustrate their opponent by attacking a variety of targets in a wide AO. Segments of the populace can play a key role in the insurgent intelligence net; in which case, they would become a primary target of friendly CI efforts.

Guerrilla forces need support from political sympathizers or foreign powers. They need an effective system of obtaining food, ammunition, weapons, equipment, and training. In some cases insurgents conduct raids for equipment. By eliminating insurgent supply nets and sources they lose combat effectiveness.

See DA Pam 381-3, How Latin American Insurgents Fight, for detailed information.

CONVENTIONAL THREAT FORCES IN LIC

Conventional threat forces in an LIC environment conduct a variety of missions. These missions involve advising and assisting insurgent forces on how to fight. Conventional threat forces train insurgents on the use of sophisticated weapons or act as leaders for insurgent units. This involvement depends on support provided by the hostile government.

Conventional threat forces can operate in traditional roles attacking and defending to support insurgents. These forces are infantry, or mechanized infantry supported by artillery, mortars, and armored vehicles. Along with limited CAS, they could have NBC weapons.

Their equipment is a mix from several major weapons-producing countries (for example, United States, Belgium, Soviet Union, China, and West Germany) . Usually this equipment is a generation or two older than that found in modern armies. However, this trend is slowly changing. The type of weapons used in an LIC environment varies from homemade weapons (mines or shotguns) to sophisticated weapons (SA-7's). Understanding the capabilities of guerrilla/insurgent weapons and collection and target acquisition systems helps you in R&S planning.

GUERRILLA/INSURGENT OPERATIONS

Guerrilla operations are those military actions executed with selected commands and combatants. For this reason, it is necessary to obtain specific enemy information, and to know the enemy's situation by observation. In guerrilla operations, attacking by surprise and having control of key terrain are essential.

FM 34-10

NOVEMBER
1986

DIVISION INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS

HEADQUARTERS DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: "Approved for public release; distribution is unlimited."

APPENDIX D

Special Operations and Environments

The geographic range of US interests in the world today requires that the division be prepared to fight and win in all types of terrain and climate.

The division may be committed to battle in areas where severe weather, climate, and terrain impact on military operations and the intelligence mission. In addition to the physical effects on the individual soldier, weapons, and equipment, environmental extremes degrade the effectiveness of IEW. Regardless of environmental conditions, the commander relies on effective IEW support. In fact, extreme environments often create a greater need for IEW support.

Special operations are those in which the natural and man-made characteristics of the area, the nature of the operations, or unique conditions under which operations are conducted may require specially trained personnel or special techniques, tactics, or equipment. Special environments include—

- ☐ Mountains.
- ☐ Deserts.
- ☐ Jungles
- ☐ Winter.
- ☐ Urbanized terrain.
- ☐ Night operations.
- ☐ IEW operations in an NBC environment.

The paragraphs below describe IEW operations in special environments. The special considerations, techniques, and procedures that will increase the effectiveness of IEW operations in harsh environments are detailed in these discussions. Special training and acclimatization periods are required for personnel to be effective in certain parts of the world. Special maintenance and operational procedures are often required to ensure IEW systems function properly. Combat operations under these conditions require special IEW support.

The effects of extreme climatic and terrain factors generally cause military operations to proceed at a slower rate than in more favorable environments. Setup and teardown times may be longer and rates of march slower. Routine functions, such as communications, can become a major undertaking. Commanders and staff officers must ensure that planning for combat operations takes into consideration the environmental influence of friendly and enemy operations.

While the means to collect data in special environments are identical to those employed in normal environments, the methods of employment and equipment used may differ.

The enemy's methods of employment and deployment will also differ, but only to the extent permitted by their doctrine or dictated by the environment.

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS IN THE MOUNTAINS

Operations conducted in mountainous areas are characterized by heavy use of indirect fires, canalized movements along valley floors, decentralized combat operations, increased collection operations from aerial resources, and reduced C^2 capabilities. Operations conducted by MI units in mountainous terrain may often result in the unit's restricted operational and sustainment capabilities.

Mountainous terrain degrades the target acquisition and early warning capabilities of GSRs and the collection capabilities of EW systems.

Because of the low density of manpack IEW equipment in the heavy division, there may be brigade areas unsupported or severely reduced in GSR and EW support. Such restrictions are minimized in light division deployments to mountainous areas because of the heavy reliance on manpacked systems in the MI battalion of the light division. Although operations may be hampered, the mission for all MI assets remains the same as in any other type operation. The optimum operation of these IEW systems in mountain terrain is affected by interrupted LOS, extreme temperature variations, and heavy precipitation.

In mountain operations, the terrain isolates friendly units, requiring them to operate more independently than in other environments. The division staff and MI battalion TOC may experience temporary interruptions in communications with subordinate units, forcing them to operate more independently and to rely on their own resources to develop the intelligence they need.

Weather in mountainous terrain is difficult to predict. The weather can change dramatically in short periods of time. As storms develop, the effects of the temperature and the windchill factor may become as important an item of intelligence as the location and activity of major enemy units. Exposed flesh can freeze in a matter of seconds. The higher elevations are frequently shrouded in rain, snow, sleet, and fog. Electronic surveillance, as well as visual observation, is severely limited under these conditions. When weather permits, mountain heights offer outstanding conditions for long-range visual observation and electronic surveillance. Weather data and forecasts are increasingly more important in selecting areas and the desired time to conduct operations.

Cross-country movement and trafficability become more important in determining enemy capabilities and intentions. Potential enemy use of nuclear weapons in mountainous terrain is a prime intelligence consideration. In some mountain terrain, the effects of nuclear detonation can be effectively contained within a specified area.

Wooded mountainous terrain has the same general effect on intelligence operations as does dense jungle. Enemy forces are difficult to detect and generally difficult to collect against. The best sources of information are EPWs, defectors, and friendly reconnaissance patrols.

Mountainous terrain favors light infantry forces. They will likely be deployed to control passes, road junctions, built-up areas, and the high ground adjacent to these areas. Enemy tactics include bypassing defensive positions and attacking from the flanks and rear. Enemy forces will decentralize the employment of artillery and use multiple rocket launchers as individual fire units.

Rugged, irregular mountainous terrain degrades AM and FM communications and associated C^2. Heavy reliance on retransmission and relay systems is required. Heavy (TACJAM) and medium (TRAFFIC JAM) ECM systems can be used for retransmission tasks when all the other means fail.

HUMINT provides the commander his best source of combat information and intelligence in this type of environment. Mountain heights offer exceptional observation post sites which are supplemented with foot patrols. Population centers in valley areas serve as lucrative HUMINT collection and interrogation sources.

OPSEC, as in all operations, will be of prime importance for attacking forces. Defending forces will have a distinct advantage to deceive and contain any attack.

EW operations suffer a definite disadvantage in mountainous terrain. Enemy communications sites use terrain masking and relay systems to thwart both DF and ECM activities. ECM and ESM systems are best employed above the valleys, concentrating on the valley floors for any enemy approaches. Ground-based signals intercept and DF systems may frequently be employed in DS of the brigades because of the dispersion of friendly forces. LOB data may

be degraded due to the terrain. Ground-based systems will normally be used in conjunction with QUICKFIX.

Mountain operations increase equipment maintenance requirements. Equipment used in mountainous environments must be rugged and man-portable. Weather in the higher elevations or during seasonal variations will affect equipment the same as in winter operations.

Reduced mobility, compartmented terrain, limited visibility, and rapidly changing weather increases the importance of reconnaissance and surveillance operations in the mountains. It is easy for the enemy to conceal his forces.

Many maps of mountainous areas are inaccurate or lack detail making terrain analysis important. Limited mobility and LOS increase requirements for aerial reconnaissance. Procedures should be established to debrief frontline soldiers, aircrews, and vehicle operators to acquire terrain information.

The mountainous environment, with severe and rapidly changing weather, limits the use and performance of aerial sensors and requires special flying techniques. Mountainous terrain complicates flight route selection. Flight routes or orbits above the ridge lines expose aircraft to unacceptable risks of detection and destruction by the enemy. Flight routes follow terrain corridors and aircraft must pop-up for limited periods to intercept or jam the target emitter or receiver. LOS is very restricted.

Mountain weather is especially hazardous to flying, particularly helicopters. The effects of fog, high altitude, wind, and ice require special consideration. See FM 90-6 for a detailed discussion of mountain operations.

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS IN THE DESERT

Deserts are semiarid and arid regions containing a wide variety of soils in varying relief. There are three types of desert: mountain, rocky plateau, and sandy or dune. Operation of EW equipment in the desert is affected by dust and sand, extreme temperature variations, static electricity, and wind.

Desert operations require highly mobile forces. The size of the areas of operations and interest are normally increased at all echelons. Collection assets are focused on targets at significantly greater distances than normal. The division may become more dependent upon corps and USAF tactical reconnaissance missions for intelligence because collection requirements may exceed the range of the division's collection capability. Extended operational areas and wide separation of combat units require more DS and GS reinforcing missions for MI resources. The mobility factor of the desert requires more tracked than wheeled vehicles for EW systems.

IPB is vital to a desert operation. Avenues of approach and mobility corridors provide for rapid movement and ample maneuever space. At the same time, visibility may be seemingly unlimited. Dust from vehicles and low-flying aircraft can be visually observed at great distances. Yet, in most deserts there are avenues of approach with some cover and concealment. IPB helps commanders use terrain to maximize mobility, cover and concealment, and effective communications. It helps them predict how the enemy will use the desert.

Desert combat is rapid. An attack may be carried out by the enemy from the line of march. Tank formations will generally be used in the first echelon and the attack may be conducted using a single echelon. The enemy may employ airborne and heliborne forces to seize objectives in the rear.

Frequent and extreme changes in desert weather have a significant influence on intelligence collection capabilities. Long periods of unobstructed visibility are abruptly interrupted by violent wind and sandstorms. These storms reduce visibility and drive sand into mechanical and electronic equipment causing frequent breakdowns. This wear and tear, particularly on mechanical equipment, requires frequent replacement of moving parts. Wide variations in day and night temperatures also have detrimental effects on both people and

machines. Precautions must be taken to prevent casualties resulting from direct exposure to the sun and to high temperatures.

High desert temperatures may cause equipment to overheat. Heat causes batteries to lose power more quickly. High temperatures cause overheating in communications equipment resulting in equipment failure. Lenses on night observation devices can become discolored when directly exposed to the sun. Communications equipment must be protected from heat and from the direct ray of the sun. Degradation of radio communications may occur due to extreme heat, while communications during hours of darkness can be excellent. During daylight, a 20 to 30 percent loss of radio communications is experienced due to heat. Frequency correcting will also limit radio capabilities. EW systems and RATT equipment will suffer frequent downtime from sand and dust if not protected. Vehicle maintenance requirements increase in extreme heat. The heat dries out seals and gaskets and causes tires to crack. The effects of sand on equipment creates the need to constantly replace bearings and other moving parts. Since reconnaissance in desert operations is generally accomplished using mobile patrols, maintenance requirements will directly impact on reconnaissance capabilities. Aerial photography and visual observation are subject to heat-wave distortion and dust storms. HUMINT operations are reduced due to smaller population areas.

OPSEC requirements increase significantly due to the long range of enemy observation and IMINT and SIGINT systems. Like OPSEC, the value of EW increases. The expansiveness of the desert precludes using terrain masking to avoid jamming. ECM can freeze the battle for destruction by fire and maneuver and plays a significant role in air defense and CAS suppression.

The QUICKFIX system and scout and air observer aircraft can be used effectively in the desert within special limits and requirements. Concealment of the aircraft is difficult. Helicopter rotors cause dust which can be seen for miles. This can be partially overcome by selecting hard-landing sites, minimizing low-altitude hovering, and treating landing zones with oil or chemicals. Nap-of-the-earth flying is essential to aircraft survival. Aircraft cannot loiter in the open for long; thus, they normally work in pairs. The desert heat reduces the lift capability of aircraft. This can be partially overcome by reducing payloads and making running takeoffs. Desert operations create additional maintenance requirements and increase the aircraft deadline rate.

Desert observations are affected by—

- ☐ Long ranges and the refraction of visible light which impairs visual perception.
- ☐ Heat waves which blur detail.
- ☐ Estimating distances due to the lack or absence of terrain reference points.
- ☐ Mirages which can distort objects to the point of being unrecognizable.

The intensity of these effects often depends on the angle of the sun in relationship to the observer. Observation in the desert is enhanced by placing observers as high above the desert floor as possible. In rolling desert terrain, tanks and other vehicles are spread over an extended area permitting observation into areas which cannot be seen by adjacent vehicle crews.

GSR and REMS are used to overcome visual distortion caused by the magnification of heat waves. In a desert environment, GSRs can be used to acquire targets at extended ranges and cover considerable distances across the front. The wide separation of combat units increases the value of GSR surveillance of flanks and gaps between units.

The optimum operation of radar in desert terrain is degraded by—

- ☐ Dust and sand.
- ☐ Temperature variations.
- ☐ Static electricity.
- ☐ Wind.

To obtain the best performance in target detection, locate the radar set as high as possible above the area under surveillance

so that the radar antenna overlooks the area. On smooth sandy surfaces, the detection range for moving targets may be reduced because sand presents a surface that does not reflect an appreciable amount of clutter. Increasing the operating angle helps to reduce this deficiency. A disadvantage caused by the terrain is that little natural cover and concealment are available for radar positions.

OPSEC and deception are vital to desert operations. Combat forces are extremely difficult to conceal in the flat, open terrain. Aerial collection platforms are very effective in locating concentrated enemy forces.

Mounted patrols are effective in desert operations. Air reconnaissance is used to the maximum extent possible. Ground reconnaissance by maneuver forces will be critical in confirming intelligence. The division's cavalry squadron is ideally suited for ground and aerial reconnaissance missions. Observation posts in static situations are sited in pairs as far apart as possible to permit accurate intersection.

The desert terrain favors wide envelopments and turning movements. Collection operations must cover all directions and use all available collection systems, especially those with long-range capabilities. Since large unit consolidations and preparations for attack are virtually impossible to hide, commanders on both sides may decide to conceal the time and place of attack through the use of deception operations. The G2 provides intelligence support for deception planning. He incorporates all of the collection means available in his collection plan to achieve as much redundancy as possible. All efforts are made to confirm or deny significant indications of enemy intentions. See FM 90-3 for a detailed discussion of desert operations.

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS IN THE JUNGLE

The jungle regions of Asia, Africa, and Central and South America are potential areas of conflict where US forces could be involved. Jungles vary from tropical rain forests and secondary growth to swamps and tropical savannas. Heavy rainfall, high and constant temperature, high humidity, and thick vegetation are the dominant features of jungle areas. These factors—climate and vegetation—contribute to restrict operational sustainment capabilities of MI units.

Because of the density of jungle vegetation, IEW operations are decentralized. Ground mobility restrictions of the jungle require all IEW systems to be light, manportable, rugged, and fielded in greater densities than in more open environments.

The jungle climate and dense vegetation reduce radio LOS and significantly reduce the effectiveness of AM and FM communications. About 10 to 25 percent of electromagnetic radiation is absorbed, decreasing communication ranges by about 20 percent. To facilitate effective command and control, hilltop and aerial relays are used. Although wire appears a logical method, security and maintenance considerations may preclude its use.

Jungle vegetation limits the identification of sounds, smells, deployments, movements, locations, and other activities which might otherwise be detected. Intense tropical storms can temporarily preclude the use of electronic collection equipment. Thick jungle terrain restricts mobility largely to roads and foot paths. The best HUMINT sources are EPWs, defectors, patrols, and the local populace. The local populace can provide a wealth of information about enemy forces operating in the local area. In insurgency situations, efforts are made to identify individuals in the area that support the enemy by providing supplies, food, and information about friendly forces in the area.

GSRs, in heavy jungle foliage, will be of limited value. Foliage distorts signal reflections from vehicles and troops passing through or behind dense foliage. Although GSR operations in jungle environments normally are limited, they are still valuable when used in a security role with other surveillance means, such as night observation devices and patrols.

Lightly equipped, long-range reconnaissance patrols play a major role in intelligence collection operations in the jungle environment. The terrain provides excellent cover and concealment, improving the chances of patrols to accomplish their mission unobserved and undetected. In patrol planning, consideration is given to the possibility that an aerial resupply, often required in jungle operations, will provide the enemy with indications of patrol activity and possibly the location of the patrol. Communications range is limited, often requiring radio relay for reporting intelligence and targeting data.

Heavy foliage and rain showers decrease the range of enemy electronic signatures, reducing the effectiveness of signals intercept. Ground-based intercept systems are concentrated in the brigade area where the enemy main effort is expected to occur. They may be used more as individual collection stations than as integrated systems. The lightweight, highly-mobile systems such as the AN/PRD-10 will find extensive use. They may accompany and support patrols.

Corps SLAR operations provide the commander with information about enemy movement. The airborne QUICKFIX has excellent radio LOS to all targets for DF intercept and COMJAM operations.

High incidents of rust, corrosion, and fungus caused by jungle moisture and humidity increase the necessity for daily maintenance on equipment especially at the operator level. This is especially true for electronic systems, which are subject to very high failure rates in jungle environments. Continuous operation of such systems generates heat which combines with moisture, corrosion, rust, and fungus to cause more frequent equipment failures.

Mountainous regions may also be found in jungle areas. These areas are particularly difficult for patrols to traverse, especially during the rainy season. In these regions, the extremes of weather can run from very hot and humid at the lower elevation to cold and wet at the highest elevations.

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS IN WINTER

Because over 50 percent of the world can become a winter battlefield, the Army must be prepared to conduct IEW operations in a winter environment. This environment is characterized by low temperatures, fog, freezing rain, snow, ice, frozen ground, and shorter periods of daylight. Spring and fall include changing weather conditions and a series of freeze-thaw cycles. The effects of the winter environment on personnel and equipment are numerous. Because of the effort and extra equipment necessary to keep warm, routine tasks take longer and are more difficult to perform. Mobility over frozen ground can be better than over unfrozen ground; snow or spring mud on the other hand, can hinder or halt movement on roads or cross country. Fog and blowing snow can reduce visibility to near zero. Performance of most electrical and optical systems is degraded.

Assessing the enemy's capability to live and fight in extreme cold is an essential intelligence requirement. Historically, Warsaw Pact forces conduct numerous exercises during the winter giving them experience in conducting combat operations in cold climates.

Snow and cold weather have detrimental effects on the operations of both mechanical and electronic equipment. The following factors can cause degradation of IEW operations:

- ☐ Reduced mobility of vehicular-mounted systems.
- ☐ Poor or inaccurate performance of radars, sensors, radios, and other electrical and optical systems.
- ☐ Antenna icing can reduce range, increase interference, alter frequency or simply collapse antennas.
- ☐ Thickened oil and lubricants can cause mechanical problems in generators and vehicles.
- ☐ Battery life decreases.

Certain environmental phenomena such as snow and fog can significantly degrade visibility making the GSR a valuable asset. However, cold weather adversely affects the performance of the GSR and must be considered by the operators. The successful operation of the radar on the winter battlefield is affected by—

- ☐ Signal scattering by airborne snow, ice, and fog.
- ☐ Variation of radar images caused by snow cover and frozen ground.
- ☐ Reduced ability of equipment operators to function in the cold.
- ☐ Reduced battery life.
- ☐ Cold and condensation-induced maintenance problems.

OPSEC is a prime consideration during winter operations. Due to the lack of live foliage in many areas, concealment and camouflage of positions, equipment, and facilities are very difficult. Vehicle and foot traffic leave an unmistakable signature in the snow. However, new snowfall can hide the noise and tracks.

Winter battlefield operations require longer to perform—even the simple tasks. Experience indicates that more time is needed for maintenance on IEW equipment.

A major impact of winter operations on equipment is caused by cold and snow. Extremely low temperatures cause metal parts of weapons to become brittle resulting in a high breakage factor for internal parts. Vehicle engines and generators require frequent starting, and the frequent starts cause condensation in the internal parts of the engine which later freezes. The intake filters of carburetors and systems are particularly susceptible to icing. Condensation on microphones and telephone handsets ice frequently if not protected. Blowing snow will also jam air intake valves. Pneumatic antenna masts and automatic data processing equipment freeze because of condensation and freezing temperatures. Power supplies have greatly reduced life spans. RATT equipment is very susceptible to malfunction under these circumstances.

Winter operations require more spare parts and oil changes. Each unit will need larger class III allocations because of frequent engine starts. Higher PLL usage factors will be experienced for filters, batteries, spark plugs, hydraulic hoses, and all types of seals. Less viscous lubrications are required.

In winter operations, the human element is all important and demands concerned leadership and thorough training. Particular attention must be given to minimizing the effects of vision whiteouts with the attendant loss of perception which affects driving and flying. High windchill factors and the potential problems of frostbite and immersion foot are additional considerations.

Only with the proper training, planning, and preparation can IEW operations be successfully conducted on the winter battlefield.

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS ON URBANIZED TERRAIN

Urbanization is gradually changing the nature of the battlefield. Urban areas, spreading across LOC and adjacent terrain, are narrowing or eliminating avenues of approach.

Urban centers may be seen as key terrain or as obstacles, depending on the nature of the conflict and the mission and capabilities of the division. Urban centers contain the bulk of the population and the economic, political, and cultural facilities of a country or area. The decision to attack or bypass an urban area may be based on political and social, as well as military, considerations. The scope of this discussion is limited to the tactical considerations for a division operating in a mid- to high-intensity conflict.

Urban sprawl expands the scope of IPB, particularly terrain analysis. It increases the requirements for detailed analysis of where smaller units can move, shoot, and communicate; and how the built-up areas

will affect both friendly and enemy organization, disposition, weapons, employment, and maneuver.

Urbanized terrain normally offers numerous avenues of approach for mounted maneuver forward of and leading to the built-up area. However, in the proximity of and within the built-up area, routes converge and become restrictive. Bypass may be blocked by urban sprawl or adjacent natural terrain.

Within the built-up areas, avenues of approach and maneuver space are determined by street patterns, building arrangements, open areas, and underground systems. Mounted forces are limited to streets, alleys, and open areas. Dismounted forces use available cover by moving through buildings and underground systems, along the edges of streets, and over roofs.

Urban combat is a three-dimensional battle. In addition to fighting at the street level, it is also conducted in the sewers, subways, basements, and in the upper stories and roofs of buildings. While this enhances OPSEC, it makes surveillance and target acquisition much more difficult.

Intelligence collection in urban areas requires intensive management. The collection effort is severely hampered by the availability of ample cover and concealment which suppress enemy unit signatures. An urban environment, particularly one that is extensive, will all but eliminate many of the indicators used to determine enemy activities and disposition. The flash, sound, smoke, and dust signatures of weapons are suppressed or distorted.

Urban areas are characterized by abundant cover and concealment and limited visibility. LOS limitations decrease the surveillance and target acquisition capability of observation posts, GSR, and signals intercept systems. Inaccurate range and azimuth readings may result when signals ricochet off buildings.

GSR will normally be deployed near the edge of urban areas used to monitor routes into and out of the built-up areas. Inside the built-up areas, radars are positioned to detect movement along streets, alleys, and open areas, especially during periods of limited visibility.

HUMINT provides the commander with the best means to gather intelligence. Troops supply first-hand knowledge about the location and type of enemy equipment and activity. Interrogations of EPWs, civilians, line crossers, and defectors will probably be the best source of information on enemy concentrations within the city. Civilians recently displaced from their homes may provide the location of enemy forces and information on structures such as fortifications, major facilities, and vehicle or foot bridges. Before the battle, HUMINT collection activity focuses on collection and analysis of city plans to support IPB of the urban area.

Communications and noncommunications intercept systems have limited effectiveness within built-up areas. There will be considerable crowding on the FM band with emitters located on tall structures to afford radio LOS. Enemy forces will make heavy use of wire and established civilian telephone systems. Manpack intercept and DF systems are well suited to support military operations on urbanized terrain (MOUT) due to their ability to be used in high towers and buildings. Vehicle-mounted ground collection systems are best used to provide early warning and indications of enemy intentions or approaches to the urban areas.

ECM also have little use in MOUT due to limited radio LOS. As with the collection assets, ECM systems are best employed to provide COMJAM support in the outlying areas along suspected avenues of approach. Additionally, ECM systems may be tasked with collection missions to support other ESM assets.

Aerial observation and signals intercept are used to overcome LOS limitations of ground-based systems. However, aerial signals intercept will still be hampered by distorted signals ricocheting off structures within the built-up areas. Aircraft flying over built-up areas can use the higher buildings for limited protection, but are vulnerable to man-portable air defense weapons from within the built-up area.

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS AT NIGHT

Both air-land battle and Soviet doctrine specify continuous combat, including combat at night and during other periods of limited visibility. Although night operations are difficult, they can be effective.

Night operations require special training, planning, and other preparation. In some cases, it requires special operating techniques and the use of night observation devices.

IEW requirements do not change significantly at night, except that a greater level of detail is needed in their planning and execution. For example, situation development requirements might include detailed information concerning enemy dispositions and terrain features.

IPB must clearly indicate where division forces and the enemy can move, shoot, and communicate. The nature and location of obstacles become more critical. Some slow-go areas may become no-go at night. Movement is slower at night. Decision points may need to be adjusted to allow more time for friendly forces to act.

Target development requirements, which are based on IPB, do not change significantly at night. However, there is a greater reliance on nonvisual means for acquiring targets. The FSE at each echelon in the division will depend more on IEW and target acquisition sensors, such as GSR, SLAR, moving target and weapon locating radars, and signals intercept for target acquisition.

Darkness affects CI requirements, particularly CI support to OPSEC. The EEFI do not change significantly, but the OPSEC measures needed to protect the EEFI do change. Noise and light disciplines are especially critical at night. Night is the optimum time for enemy patrols and agents to infiltrate and exfiltrate. Since night is also the time that friendly patrols are most frequently used, the coordination of routes, passage points, passwords, and other recognition signals is vital.

Deception is easier at night. But this is a two-edged sword. While the division can use darkness to deceive the enemy, the enemy will likewise use this opportunity to deceive the division commander. The division intelligence system must employ other collection means to compensate for the lack of visual confirmation.

HF communications signals, due to changes in the atmosphere, travel farther at night. This results in more unintentional jamming on division HF nets. HF radio operators must be more alert to unintentional jamming which the enemy might attempt to slip in with other interference. Use of directional antennas, which is important in all battlefield conditions, is especially critical at night. At night, more information must come from signals intercept operations due to degraded HUMINT capabilities.

While night operations have little effect on the capability of IEW systems, it does affect how they are employed. Some IEW sensors can help overcome the limitations imposed by darkness. GSRs are especially useful at night. This is especially true of the AN/PPS-15 radar, whose range approximates that of visual observation. GSRs and night observation devices used together in a mutually supporting role are very effective. GSRs can be used in other ways to compensate for the darkness. They can vector patrols and movement of other forces which have greater difficulty navigating at night.

While darkness provides protection for IEW systems, it also imposes special requirements. IEW teams must reconnoiter operational positions, ingress and egress routes, and enemy approach routes into positions during daylight when possible. This reconnaissance must include supplementary and alternate positions. IEW teams must train to emplace, displace, move, and operate their equipment at night.

MI units should habitually train with fire and maneuver units during night operations. Darkness increases the need for coordination.

IEW SUPPORT OF THE NIGHT ATTACK

The division attacks at night to gain or maintain the initiative, exploit daylight success, and to overcome certain disadvantages, such as—

- ☐ Inferior combat power.
- ☐ Enemy defensive obstacles and fortifications.

Detailed information and intelligence about the enemy and terrain is needed to support a night attack. Daylight reconnaissance provides the following information:

- ☐ Enemy positions.
- ☐ Obstacles and bypasses.
- ☐ Weak points or gaps in the defensive sector.
- ☐ Assembly areas, routes of advance, assault positions, and objectives.
- ☐ Landmarks to enhance control of the attack.

When time permits, a night reconnaissance is also conducted. However, the location and time of attack must not be compromised.

Surprise is a primary objective of a night attack. OPSEC during preparation for the attack is vital. Movement to and displacement from assembly areas is a critical phase of the operation. The division may plan and execute a deception operation to confuse the enemy concerning the division commander's intentions and the time and place of the attack. A well planned and executed night attack is not discovered until the assault has begun.

Attacking elements of the division use GSRs and night observation devices to observe the enemy and his activities during the attack. Night observation devices assist in navigation and avoidance of obstacles. Radars may be oriented in the direction of the attack and provide direction to the attacking force.

IEW SUPPORT OF THE NIGHT DEFENSE

The night defense has all the elements of a daylight defense. Defending division forces must deny the enemy the use of darkness to gain the element of surprise. They integrate IEW sensors, night observation devices, and patrols into a surveillance plan.

Division units conduct a daylight reconnaissance prior to or upon occupying defensive positions. The reconnaissance should—

- ☐ Determine avenues of approach into the defensive sector.
- ☐ Detect enemy preparation for attack, including reconnaissance activity.
- ☐ Identify good ambush sites along avenues of approach into the division sector.

IEW sensors, night observation devices, patrols, and illumination devices enhance the effectiveness of the night defense. Radars support friendly reconnaissance patrols and provide early warning to listening and observation posts concerning enemy movement. GSRs are reinforced with night observation devices. Together, they provide overwatch of obstacles and barriers. Remote sensors are employed along avenues of approach and defilade areas. USAF tactical air reconnaissance and SLAR missions provide early warning and detection of enemy assault and follow-on forces.

OPSEC is a critical factor in the night defense. OPSEC measures include noise and light discipline. COMSEC and electronic security must be strictly enforced. Generators are dug in and sandbagged to reduce their signatures.

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS IN A NUCLEAR, BIOLOGICAL, AND CHEMICAL ENVIRONMENT

The MI battalion commander and his staff must consider how NBC weapons will affect operations. Enforcement of the three principles of NBC defense will enhance the survivability and effectiveness of MI operations. They are—

- ☐ Contamination avoidance.
- ☐ Protection.

- Decontamination.

CONTAMINATION AVOIDANCE

Contamination avoidance is the best way to minimize the impact of NBC weapons. It involves implementing passive defense measures, using the NBC warning and reporting system effectively, NBC reconnaissance, minimizing exposure, and avoiding known NBC hazards.

- Passive defense measures use NBC monitoring and detection equipment, chemical protection covers, and friendly vulnerability analysis techniques to avoid being targeted.
- Key leaders of the MI battalion formulate NBC reports and interpret reports received.
- Battalion and company NBC reconnaissance teams rapidly disseminate locations of NBC hazards for movement planning.
- Crews rotate and use protection shelters and available cover to minimize exposure to NBC hazards.
- Avoiding NBC hazard areas is the best course of action. This will minimize degradation caused by the use of protective equipment and negates the need for decontamination. FM 3-3 describes how units can avoid excessive contamination in the NBC environment and FM 3-4 describes means for protecting troops from NBC contamination.

In the event the MI battalion elements are forced to operate in a contaminated area or are operating where the threat of NBC attack is high, effective use of NBC protection, both individual and collective, is critical. The commander and his staff must be aware that use of protective equipment, while critical for survival, will result in degradation of mission effectiveness because—

- Use of individual equipment will result in excessive heat stress, loss of manual dexterity, visual acuity, and fatigue.
- Time needed for mission accomplishment will increase based on factors of fatigue, training, level of protection and weather. FM 3-4 contains estimated times for accomplishing tasks while in mission-oriented protective posture (MOPP) 4.
- Collective protective systems retrofitted to MI systems restrict operations. Entry and exit procedures must be followed to avoid contaminating the interior.
- Logistical requirements for the exchange of overgarments, rations, and water expand drastically. Approximately 13 quarts of drinking water per soldier per day is required to prevent dehydration during extended periods of MOPP 4 (see the following illustration for MOPP levels).
- Extensive training in MOPP analysis is required as MOPP-level selection is delegated to the lowest level possible.
- Extensive peacetime training and acclimatization is required as all members of the battalion must be capable of performing mission tasks while in MOPP 4.

Commanders and leaders must be aware that if forced to operate in MOPP 4—

- Personnel and equipment will be stressed to a greater level than normal.
- Times to accomplish IEW mission will increase.
- The logistical and maintenance burden will increase.

DECONTAMINATION

Decontamination is the reduction of the hazard to a level necessary to continue the mission. The MI battalion is responsible for the hasty and deliberate decontamination of its troops and equipment using battalion decontamination equipment.

MOPP LEVELS

LEVEL	OVERGARMENT	OVERBOOTS	MASK/HOOD	GLOVES
1	WORN*	CARRIED	CARRIED	CARRIED
2	WORN*	WORN	CARRIED	CARRIED
3	WORN*	WORN	WORN*	CARRIED
4	WORN	WORN	WORN	WORN

*In hot weather, the coat or hood can be left open for ventilation.

MOPP O - Soldiers carry the protective masks with load-carrying equipment, and the MOPP gear is readily available (that is, within the work area, vehicle, fighting position, or the like).

MASK ONLY* - Soldiers do not need to wear protective overgarments or rubber gloves as long as they are protected from direct skin exposure to liguid or solid contamination (transfer hazards).

*MASK ONLY is inappropriate when a blister agent is present.

Complete decontamination to peacetime levels is impossible due to absorption/ desorption. Decontamination is very time-, material-, and labor-intensive. Divisional NBC defense units will be tasked to assist divisional units. Company teams will have to depend on support from the battalion decontamination team and the supported brigade. For a more detailed description of decontamination, consult FM 3-5.

NUCLEAR CONSIDERATIONS

Three specific nuclear weapons effects will have a severe impact on electronic equipment utilized by the MI battalion. These effects are—

- Electromagnetic pulse (EMP). A sharp pulse of radio frequency (long wavelength) electromagnetic radiation produced when an explosion occurs in an symmetrical environment, especially airbursts. The intense electric and magnetic fields can damage unprotected electrical and electronic equipment over a large area.
- Transient radiation. Transient radiation effects on electronics (TREE) which are caused by gamma radiation given off by a nuclear detonation.
- Blackout. A temporary loss of communications due to the mechanical disturbance of the atmosphere caused by a nuclear detonation. This effects communications systems which use omnidirectional antennas.

EMP and TREE mitigation techniques will reduce the harmful effects of nuclear effects on MI unit operations. EMP mitigation techniques are employed for the protection of communications and key electronic collection systems. During periods of increased probability of the enemies' use of nuclear systems, redundant systems that can be shut down should be. All antennas on dormant systems should be removed. Shield the overall system by closing doors to shelters, air intakes, and any other openings. Stress the use of proper grounding techniques. Star grounds are best for EMP protection. Grounds and other wires should not cross or form loops.

TREE mitigation techniques include reset and alternative communication means:

- Reset or reload computer systems after nuclear detonations, maintain duplicate programs and data bases off line, and shield handheld and duplicate calculators.
- Under blackout conditions, use wire or messengers until electronic communications systems are restored to use.

For a more detailed description of EMP mitigation techniques, consult FC 50-16.

The effects of blast, thermal, and nuclear radiation must also be considered in terms of personal vulnerability and material damage. FCs 50-15 and 50-20 provide additional information concerning survivability and mitigation.

Glossary

A

A^2C^2	Army airspace command and control
ACofS	Assistant Chief of Staff
ACR	armored cavalry regiment
ADA	air defense artillery
ADC(O)	assistant division commander for operations
ADC(S)	assistant division commander for support
ADE	assistant division engineer
adj	adjacent
AE	aerial exploitation
AM	amplitude modulated
AMC	US Army Materiel Command
AME	airspace management element
anal	analysis
AO	area of operations
APOD	aerial ports of debarkation
ARTEP	Army Training and Evaluation Program
arty	artillery
AS	aerial surveillance
ASI	additional skill indicator
ASPS	all-source production section
at	antitank
ATE	automatic test equipment
Aug	August
AVIM	aviation intermediate maintenance
avn	aviation
AVUM	aviation unit maintenance
AWOL	absent without leave
AWS	air weather service

B

BAI	battlefield air interdiction
bde	brigade
BMCT	beginning of morning civil twilight
bn	battalion
BOMREP	bombing report
BSA	battalion support area
BTF	battalion task force

C

C^2	command and control
C^3	command, control, and communications

FM 34-3

INTELLIGENCE ANALYSIS

MARCH 1990

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: **Approved for public release: distribution is unlimited**

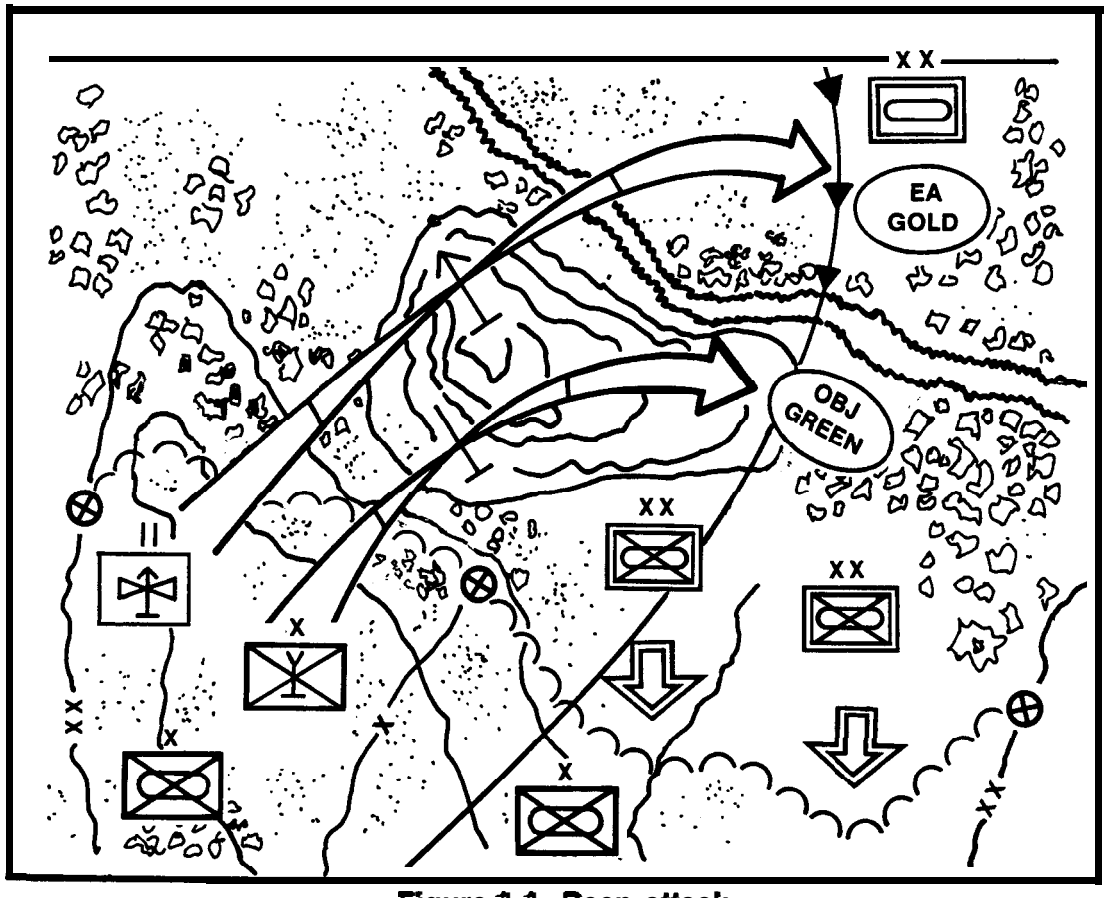


Figure 1-1. Deep attack.

using the weather and the terrain, the friendly commander can successfully defeat a superior enemy force.

To gain the initiative, the commander must--

- See the enemy early and determine the capabilities and intentions of the enemy.
- Find and track enemy follow-on echelons.
- Identify enemy high-value targets (HVTs), targets which if successfully attacked, will contribute to the degradation of important enemy battlefield functions,
- Identify, locate, and develop the required targeting data for the attack of HPTs, which if successfully attacked, will contribute to the success of friendly plans.
- Detect enemy weaknesses and develop the necessary data to support the exploitation of these weaknesses.

- Effectively use electronic warfare (EW) to support the AirLand Battle while protecting friendly use of the electromagnetic spectrum.

- Determine the enemy's capability and guard against that capability.

- Protect friendly forces and operations from enemy intelligence collection operations.

- Use the weather and terrain to friendly advantage.

IEW support is vital to the successful planning and execution of the AirLand Battle at all echelons. Intelligence support at brigade and battalion levels focuses primarily on the close operation, while at division it focuses on both close and deep operations. Corps is the focal point for intelligence operations that support rear and deep operations.

Intelligence support of close operations supports the commander's risk analysis and consideration of mission, enemy, terrain, troops available, and time (METT-T). As such it must be the first step in planning. Intelligence operations reduce risk by identifying the enemy's most likely courses of action, and so al low the commander to concentrate or disDerse forces as appropriate. Intelligence also provides administrative and logistic personnel, engineers, air detense artillery (ADA) staffs, and other planners with guidelines about the expected situations and enemy so they may make the best use of scarce assets.

To conduct deep operations the intelligence system supports the . . commander's need to look deep, find and follow enemy follow-on forces, and detarmine their capabilities, vulnerabilities, and intentions. The commander must designate the HPTs and decide where and when to attack them to achieve the greatest benefit to the operation. The commander conducts deep attacks against designated HPTs to '"shape'" the battlefield by forcing the enemy commander to deviate from established plans and to create favorable conditions for friendly commanders conducting close operations. To facilitate deep operations, corps-level intelligence planning must focus its attention on analyzing and estimating enemy capabilities, intentions, and likely courses of action at least 72 hours in advance. At division-level, intelligence planners must perform this same function at least 24 hours in advance.

Intelligence support of rear operations supports the commander's need to identify enemy capabilities, intentions, and likely courses of action to interdict friendly combat support (CS) and combat service support (CSS) functions, and to inhibit the ability of the friendly commander to flexibly employ the reserves. The intelligence planner must consider all means and measures available to tha enemy, to include sabotage, unconventional warfare, airmobile or airborne assaults, nuclear, chemical, and conventional long-range strikes, deception, and the employment of maneuver forces in deep exploitation or raiding operations.

THE BATTLEFIELD AREA

Commanders consider the battlefield in terms of the time and space necessary to defeat an enemy force or complete an operation before the enemy can reinforce. They view the battlefield as having two distinct areas: the AO and the area of interest (AI).

The AO is that portion of an area of conflict necessary for military operations. The AO is assigned by the next higher commander and designated by lateral and rear boundaries. It carries with it the authority and responsibility to conduct operations therein. The commander must coordinate with adjacent commanders before conducting maneuver and fire support (FS) activities outside the designated AO.

The AI is that area of concern to the commander which includes the AO and areas adjacent thereto. It includes areas forward of, and to the flanks and rear of the AO. It encompasses areas either occupied by enemv forces that could jeopardize friendly mission accomplishment and/or which includes the objectives of friendly current or planned operations.

Each commander determines his own AI. The commander generally relies on higher headquarters and adjacent units to provide information and intelligence about enemy forces in that area. Figure 1-2 shows the battlefield areas of division.

Battlefield areas are important to the intelligence analyst because they help focus the information requirements of commanders concerning the weather, terrain, and enemy forces from battalion to echelons above corps (EAC). Specific information requirements are dependent on the mission and the tactical situation. Usually, in conventional operations, information requirements (IR) on enemv forces are based on the one-up and two-down formula. Commanders require detailed information about enemy forces at their equivalent levels of command as well as at one level above and two levels below their own. For example, brigade commanders need information about enemy regiments (equivalent level), enemy divisions (one-up), and enemy battalions and companies (two-down). Generally, the enemy forces of concern to each commander are found within the command's AO and AI.

The IEW mission includes four major tasks: situation development, target development, EW, and counterintelligence (CI).

Situation development (discussed in Chapter 6) provides commanders with the intelligence they need to make sound tactical decisions. It is a continuing estimate of the situation that projects enemy intentions and the effects of the weather and terrain. Situation development helps cormnanders--

- Find and follow enemv forces.
- Determine enemy capabilities, vulnerabilities, and intentions.
- Identify the enemy main effort.

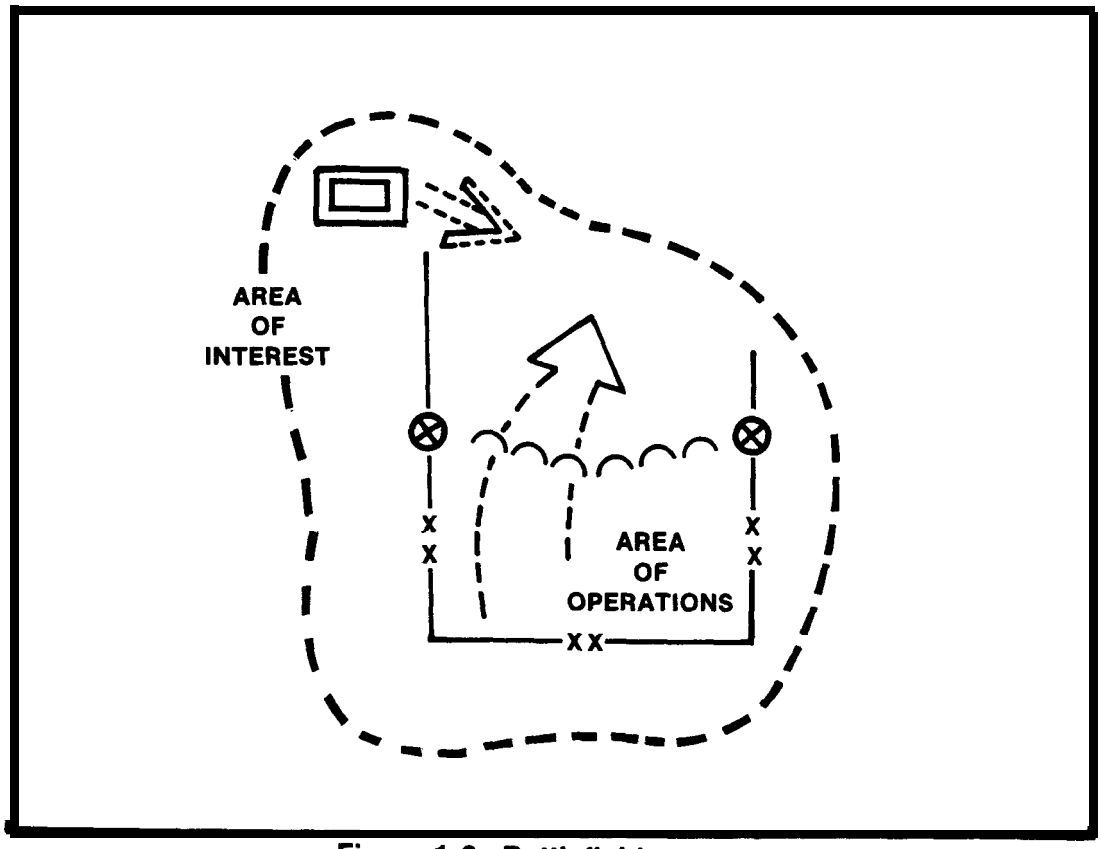


Figure 1-2. Battlefield areas.

- Determine how the weather and terrain will affect friendly and enemy operations.
- Detect opportunities to exploit enemy weaknesses and seize or retain the initiative.
- Assess the relative value of enemy combat systems, which serves as a basis for selecting HVTs.

Target development (discussed in Chapter 7) provides combat information, targeting data, and correlated target information which support the commander's tactical plans. It focuses on HPTs which have been selected, through the targeting efforts of the G2 or S2, the G3 or S3, and the fire support element (FSE), and approved by the commander. Target development identifies, locates, and tracks HPTs until thev are neutralized. Target development operations must provide sufficiently accurate targeting data to attack by fire, maneuver, or electronic means.

Situation and target development provide the intelli gence required to fight the AirLand Battle. Both are distinct tasks, but are interrelated and totally integrated to provide an accurate picture of the battlefield.

EW (discussed in Chapter 8) exploits, disrupts, and deceives the enemy command and control (C^2) system while protecting friendly use of communications and non-communications systems. It is a significant force multiplier when integrated and employed with fire and maneuver. EW consists of the following functions:

- EW support measures (ESM), which provide commanders the capability to intercept, identify, and locate enemy emitters.
- Electronic countermeasures (ECM), which provide commanders the capability to disrupt enemy use of the electromagnetic spectrum.
- Electronic counter-countermeasures (ECCM), which are used to protect friendly command, control, and communications (C^3) systems against enemy radioelectronic combat (REC) activities.

CI (discussed in Chapter 9) includes specific actions which support the protection of the friendly force. Enemy commanders, to succeed against friendly forces, must employ all-source intelligence systems to collect information about friendly forces. Depriving enemy commanders of vital information about friendly forces is crucial to friendly success on the battlefield. CI enhances the operations security (OPSEC) of the command by supporting the following actions:

- Countering the hostile intelligence threat.
- Safeguarding the command from surprise.
- Deceiving the enemy commander.
- Countering enemy sabotage, subversion, and terrorism.
- Developing essential elements of friendly information (EEFI).

THE INTELLIGENCE ANALYSIS SYSTEM

The intelligence analysis system is a single, integrated system that extends from battalion level to national agencies. Figure 1-3 shows the all-source intelligence system.

The system includes the directors, coordinators, producers, and executors. All are linked together both laterally and vertically to ensure a coordinated and effective effort. Figure 1-4 shows the common IEW structure.

Analysis elements are the heart of the intelligence system. They include--

- Intelligence officers and their staff sections.
- Echelons above corps intelligence centers (EACICs).

DETERMINING THE RISK FACTOR

Uncertainty is what the job of intelligence is all about. To succeed, the analyst handles uncertainty from a number of sources. While objective ground truth is found in the laboratory, it is not part of analysis of the battlefield. The analyst frequently deals with ambiguous or even misleading information.

The analyst's greatest concern is uncertainty, the commander's is risk. Good analysts translate uncertainty into risk. Figure 5-2 shows a graph of risk functions to consider. Risk increases as enemy lethality moves from low to high. When a range of uncertainty is added to the estimate of lethality, the potential danger becomes even greater. The degree of risk a commander will accept governs the amount of uncertainty the analyst reports.

For example, under a very high level of uncertainty, the commander faces between one and three enemy tank divisions. The analyst admits the level of uncertainty involved, while collecting and processing information to reduce the uncertainty. The level of uncertainty that the analyst

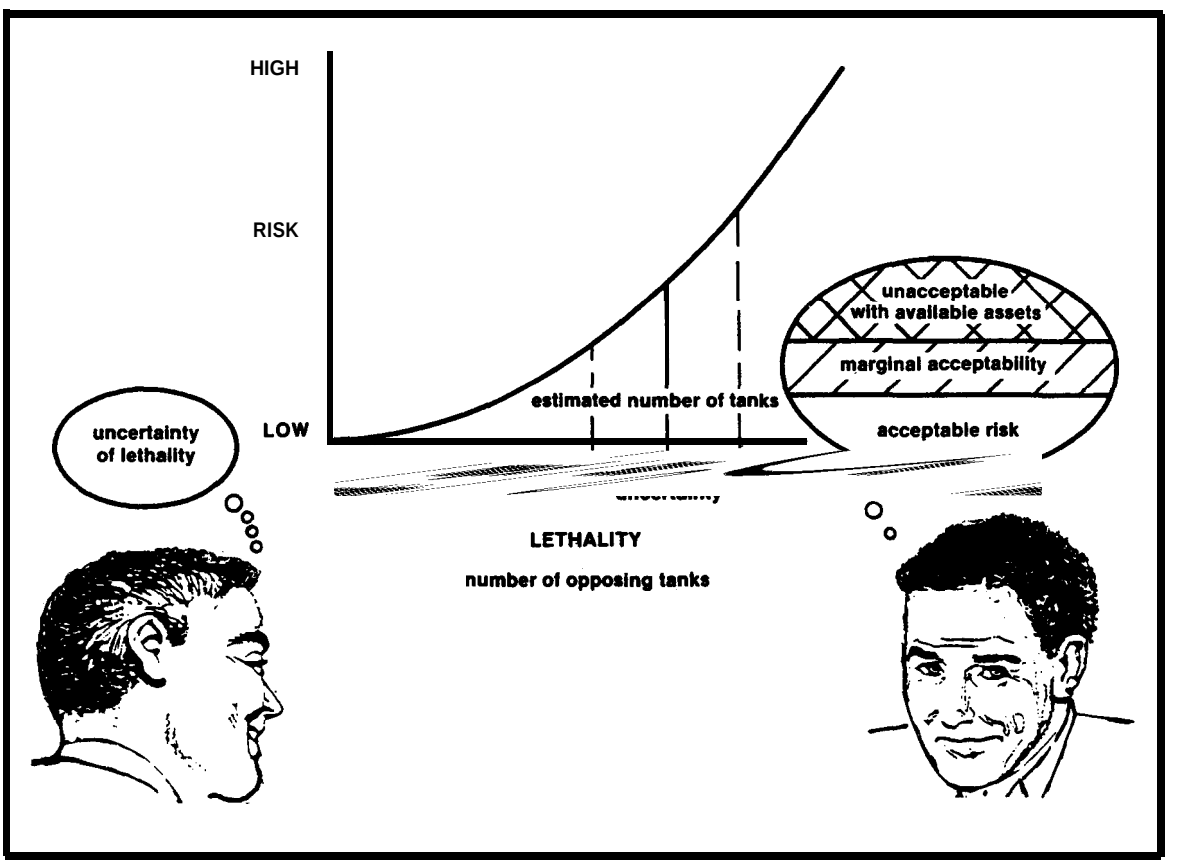


Figure 5-2. Translating uncertainty to risk.

accepts is driven by the degree of risk the commander accepts. The commander is unable to properly plan for battle knowing only that friendly forces face "between one and three enemy tank divisions". The same commander is not concerned about facing 10 or 12 enemy tank battal ions; the commander employs the same plan regardless, in facing 10, 11, or 12 battalions. The analyst does not waste time reducing the level of uncertainty beyond reporting "1O to 12 tank battalions" because the commander is satisfied with the given degree of risk.

Risk is a voluntary exposure to danger, however unavoidable it might be under the circumstances. In combat, there is always risk in not preparing response to a potential enemy action whether or not that action has a high possibility of execution. Risk increases in response to potential danger and decreases when the enemy threat credibility goes down.

Risk increases when--

- Enemy force lethality increases.
- Warning time decreases. (Crises occur when warning time is less than the required preparation time; the worst-case situation is when there is total surprise and no warning.)
- The number of enemy options increases. (If the enemy's plans are ambiguous, then friendly forces might not plan effective responses to all of the enemy opt ions.)
- The number of friendly options decreases. (If fewer options are available for countering the threat, there is a greater chance that the available options will not work.)
- The enemy's knowledge of the battlefield environment, including friendly forces increases.

Risk decreases when--

- The enemy force lethal ity decreases.
- There is greater warning time.
- The enemy has fewer options.
- The number of friendly force options increases.
- The friendly force knowledge of the battlefield environment, including enemy forces, increases. Knowing how the environment affects combat operations allows the commander to exclude unworkable courses of action and to gain maximum effectiveness from others.

The analyst's uncertainty plays a key role in the evaluation of the enemy and the amount of risk accepted. Uncertainty may arise for many

reasons. First, there is uncertainty about the enemy's intent: "What is the enemy's real objective? What are the various means of achieving this objective?"' Second, there is uncertainty in evaluating the capabilities of the enemy force to achieve these objectives. Third, there is uncertainty in other factors (lethal ity, warning time, enemy and friendly options, and environmental conditions). Fourth, there is uncertainty that the method of response will produce the desired outcome.

THE THREAT MODEL

The threat model is a portrayal of the enemy. It allows the analyst to piece together information, identify information gaps, speculate and predict, and do problem solving. Most importantly, the threat model allows some of the risk in a given situation to be quantified. There will always be inaccuracy in a model, and so there will always be uncertainty. Still, based on the model, an analyst can look for changes in a real-world situation to identify patterns, trends, and activity levels. Creating such a model requires a knowledge of--

- Physical objects such as weapons, vehicles, and radar.
- Organizational structures of enemy and friendly forces.
- Battlefield environment, including terrain, hydrology, and weather.

Once developed the model is refined and maintained, or it will lose its validity.

Threat models incorporate white elements (battlefield geography and environment conditions), red elements (the enemy force (or threat), and blue elements (the friendly force). The three elements of white, red, and blue form an organizational structure from which the analyst can mentally picture the battlefield. Figure 5-3 illustrates elements of the threat model.

Thinking white is understanding the elements of the environment as they affect the battle. In threat modeling, development of the white framework comes first. It is the white framework that anchors the threat model to the real world. The white framework is made up of space and time.

Developing the geographic framework of the battlefield is as simple as plotting the battlefield on a map. The dimensions of the battlefield encompass the unit's AO and AI.

The map is a model of the real world. The topographic map contains a wealth of information about the battlefield environment, including descriptions of terrain, roads, and population centers. The highly detailed military map contributes more information to the threat model.

Time in the threat model is a sequence of time-period snapshots (or windows) within which events occur. The analyst compresses threat model

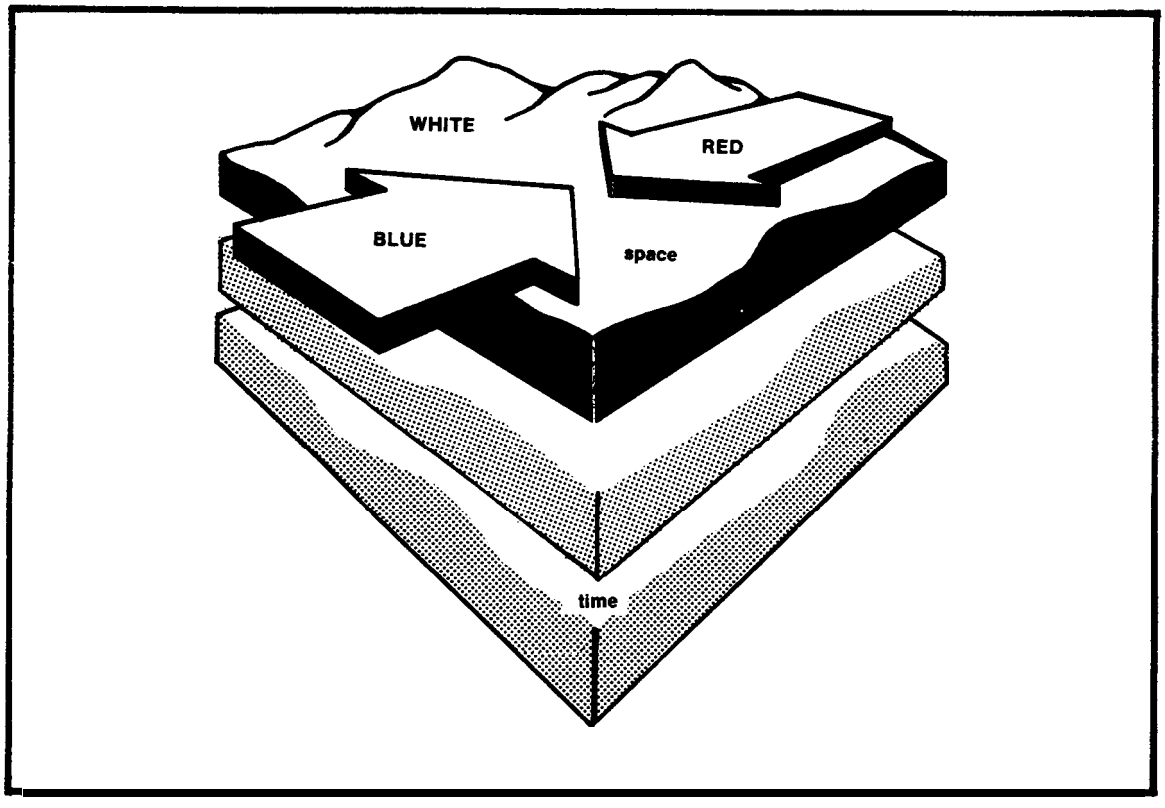


Figure 5-3. Elements of the threat model.

time to bring events closer together or expand it to make individual events more distinguishable. Overlaying time windows helps in seeing patterns of events or distinguishing changes. In the threat model snapshot sequence, one of the snapshots represents the current time frame. A sequence of snapshots al lows the analyst to fol low courses of action from the current time frame to the eventual outcome of the battle. Each snapshot represents an overlay of information on the battlefield geography. Figure 5-4 shows this.

Thinking red is seeing the battle from the enemy's viewpoint. The red element of the threat model is anchored in the real world. Enemy forces use the political and military policies of the foreign nations involved. The enemy combat force is an extension of political policies that are the source of the conflict that creates the battlefield situation.

Next, in threat model ing, plot the red element, including locations and likages of the political, military, and combat organizations on the battlefield. The highest echelon of enemy organization plotted depends on the echelon of interest to the friendly force commander. For example, the strategic-level threat model has all aspects of the civil ian and mil itary

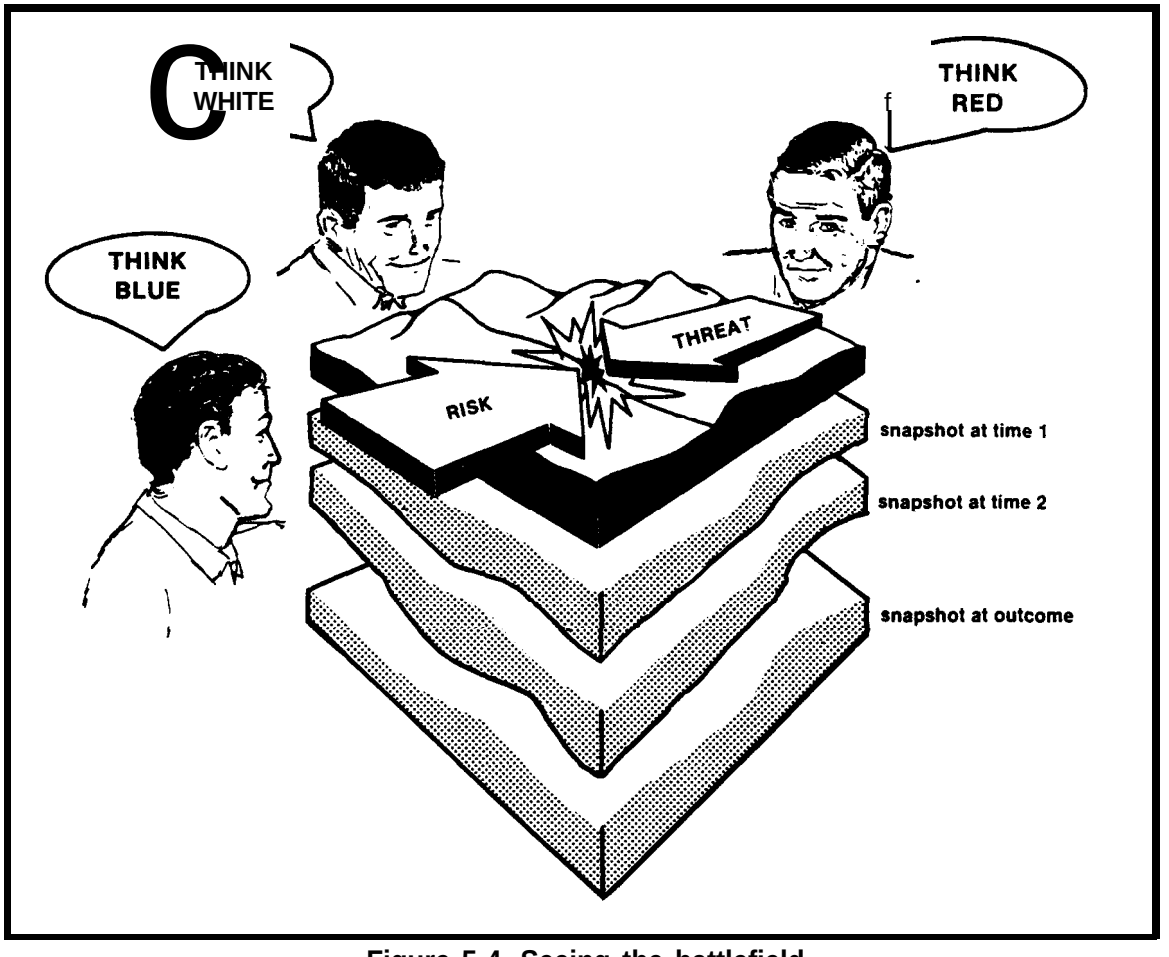


Figure 5-4. Seeing the battlefield.

force structure, whereas a division-level threat model shows only the locations of the red forces up to army level.

The organization of red elements follows some form of hierarchical structure, connected by lines of communication (LOC). The LOC shows the relationships between units for command, control, and coordination. The LOC is overlaid on the geographic structure and relates to physical communication paths like roads, transmission lines, or electromagnetic transmission paths. Figure 5-5 shows the three techniques.

Thinking blue refers to seeing the battle from the friendly commander's point of view. The threat model takes on its full meaning when the blue element is introduced along with white and red. The targets of red threat are blue elements; the components of the friendly force are blue elements.

Fill out the RED War Plan with three techniques:

1. **Start with enemy doctrine to structure the war plan.**
2. **Exploit intelligence sources to fill in details.**
3. **Use analogies to fill in missing information.**

Figure 5-5. Red elements three techniques.

The most common failing of analysts is their inability to "think blue". Analysts become extremely knowledgeable about the enemy, knowing nearly exact numbers of equipment, biographies of commanders, and unit histories, but they cannot see how friendly forces operate. It does little good to understand enemy aviation without understanding some of the characteristics of friendly air defense. While there are staff officers who are experts in friendly systems and tactics, the analyst must still have a familiarity with blue doctrine and tactics. This returns to the need for a shared conceptual model.

In plotting the location of units in the white framework, the analyst is concerned with the location of those combat units that information from the threat model supports. Figure 5-6 lists some information sources for developing the blue element of the threat model.

- **Operations plan for the friendly force.**
- **Friendly force doctrine.**
- **Mission plans.**
- **RED view of friendly forces.**
- **Situation reports from operational elements.**
- **Mirror imaging.**

Figure 5-5. Information sources for developing the blue element.

Figures 5-7, 5-8, and 5-9 show checkl ists of white, red, and blue questions that are asked when creating the threat model.

What is the geography of the battlefield?

What is the culture of the country area?

What is the history of conflicts in this region?

What is the attitude of the local population toward the enemy force? toward the friendly force?

What is the academic, economic, and technological level of the local population?

How is the local population armed?

How is the population distributed in the region?

What local cultural features (airfields, railways) can be exploited for military purposes?

How predictable is the weather in the area?

How does the weather affect operations, personnel, trafficability, equipment, and communications?

During what time frame will hostilities occur?

How much time is available for preparation?

Figure 5-7. Checklist of white questions.

What is the enemy's doctrfne?

What are the enemy's tactics?

How does the enemy prepare war plans?

How does the enemy train?

What are the enemy's objectives?

How is the enemy equipped?

What is the enemy's strategy?

How is the enemy force sustained?

What are the enemy's operational plans?

How is the enemy force structured?

What are the enemy's courses of actions?

Figure 5-8. Checklist of red questions.

What are the BLUE principles of war?	What resources does the have at his disposal?
What are the friendly objectives?	What are the priority information needs of the commander?
What are the friendly force resources?	What are the information needs to execute the mission?
What is the commander's mission?	

Figure 5-9. Checklist of blue questions.

Given a model of how the battlefield should appear in a certain situation, the analyst develops and tests hypotheses of how the enemy may act. An hypothesis is an explanation that accounts for a set of facts and that can be tested by further investigation. It is a set of logically related propositions and an outcome. An hypothesis can be proven false based on evidence, but it can never be proven correct in advance. The best that the analyst can do is rank order several hypotheses or assign rough probabilities to them, Whan seeking evidence to support or reject a hypothesis there are several considerations for the analyst:

- The enemy can be engaged in deception. The course of action selected by the enemy does not have to be the best, but only adequate. Deception efforts then can be mounted which support the most obvious course of action.
- Sensors can collect only in the areas where they look. If targeted at one specific area, they may not collect information in another. This information not collected may have confirmed or denied a particular course of action.
- Indicators may be redundant to several hypotheses,
- Several sensors may collect the same piece of information. This can give undue weight to a hypothesis.
- Some small indicator may be vital to a certain course of action. Large scale river crossings, for example, require engineer support. If that support is conclusively absent, a river crossing cannot occur, no matter what else supports that hypothesis.
- The evidence gathered in one area may not be representative of the whole battlefield. For example, the enemy has 15 battalions of artillery available. Sensors report 4 battalions in the north and 2 in the south. This does not conclusively indicate a total of 10 battalions in the north and 5 in the south. The true disposition may be 4 in the north and 11 well camouflaged battalions in the south .

When selecting an hypothesis as "most likely" or rejecting it out of hand, all of the above issues come into play. These errors in thinking may lead to false alarms or rejecting perfectly good ideas. Other errors also exist which affect analysis. They are called biases.

BIASES

If a single term best describes the factors that interfere with successful analytic thinking, it is bias. A bias is a subjective viewpoint. It indicates a preconceived notion about something or someone. Analysts must recognize biases and be aware of the potential influence they can have on judgment.

Biases can have a positive influence on analysis. With a iack of information, a preconceived notion gives a starting point for thinking about a situation. However, biases are generally bad because they obscure the true nature of the information. The analyst must recognize several categories of biases so as not to be misled or drawn into the wrong conclusions during the analysis process. Biases are cultural, organizational , personal, and cognitive (perception).

CULTURAL BIASES

Cultural biases begin forming at an early age and continue throughout a lifetime. They interfere with the ability to think in the same manner as the enemy (think red). Analysts need considerable background information on culture and social mores to perceive a situation In the same way the enemy perceives it. If analysts do not have this experience or information and decide to depend upon their own values when looking at a situation, the analysis is likely to be wrong. The reason for this is that different cultures tend to view similar situations differently.

ORGANIZATIONAL BIASES

Most organizations have specific policy goals. Any analysis done within these organizations may not be as objective as the same type of analysis done outside the organization. Some of the problems that occur from a subjective internal analysis range from an unconscious altering of judgment because of exposure to selective information and common viewpoints held among individuals, to deliberately altering a judgment to provide what the commander wants to hear. "Best case" analysis is a good example.

"Best case'" is where an analyst preeents the situation in the most optimistic light so as not to anger the commander. This frequently underestimates the enemy's capability while overestimating friendly capability.

PERSONAL BIASES

Personal biases come from past experiences. If a thought pattern previously led to success, analysts may continue to follow this pattern.

Even if the situations have nothing in common, the tendency to follow the methods that were successful in the past is very strong.

COGNITIVE BIASES

The all-source analyst evaluates information from a variety of sources (including HUMINT, SIGINT, IMINT, and open sources). Each source has strengths and weaknesses. The degree of reliability, completeness, and consistency varies from source-to-source and even from message-to-message. This variance often creates doubt about the reliability of some sources.

The cognitive biases that cause analysts the most problems are vividness, absence of evidence, oversensitivity to consistency, persistence of impressions based on discredited evidence, and availability.

Vividness

Clear and concise information has a greater impact on thinking than abstract and vague information. Even if the vague piece of information has more value as evidence, the tendency is to disregard faster than you would eliminate a clear piece of information.

Absence of Evidence

Lack of information is by far the most common problem, especially in a tactical environment. This does not mean that analysts should be content with the information on hand; they always want more. Analysts shouldn't hold back information because it is not conclusive. It rarely is. Instead the analyst should--

- Realize that information sometimes is missing.
- Identify areas where information is lacking and consider alternative hypotheses.
- Adapt and adjust judgments as more information comes in.
- Consider whether a lack of information is normal in those areas or whether the absence of information is itself an indicator.

Oversensitivity to Consistency

Consistent evidence is a major factor for confidence in the analyst's judgment. On the one hand, consistent information is appropriate. On the other hand, information may be consistent because it's redundant, or it may come from a small or biased sample. The analyst considers if the evidence is representative of the total potentially available information. If it is not, or if it is not known, then the confidence level is low, regardless of the consistency. The analyst must be receptive to information that comes in from other sources regardless of whether it supports the hypothesis or not.

Persistence of Impressions Based on Discredited Evidence

Whenever the analyst receives evidence, there is a tendency to think of things that explain the evidence. These connections create impressions. Although the analyst discredits the evidence, the connection remains, and so do the impressions. An example is a clandestine source under hostile control. If the source has a record of passing accurate information, the analyst tends to judge all information that is passed according to previous accuracy. The analyst may doubt the validity of the report claiming that the source is under hostile control or may rationalize the inaccuracy in some other way. Either way, the evidence is based on previous information and not on current indicators. This is one way an enemy could launch a deception operation. This is important. An analyst who "reasons away" information contrary to pet hypotheses does the commander a disservice. Analysts must be professional and capable of saying, "I was wrong," before the situation is lost.

Availability

The ability to recall past events influences judgment concerning future events. Since memory is more readily available, and is more acceptable, it is easy to rely upon memory instead of seeking a proper sample to predict events.

Overcoming bias is a vital step to proper analysis. Any of the above biasas reduces the quality of analysis performed.

CHAPTER 6

SITUATION DEVELOPMENT

Situation development enables commanders to see and understand the battlefield in sufficient time and detail to make sound tactical decisions. It helps locate and identify enemy forces; determine their strength, capabilities, and significant activities; and predict their probable courses of action. Situation development helps the commander to effectively employ available combat resources where and when the decisive battles will be fought. Also, it helps prevent the commander from being surprised.

This chapter describes the analysis phase of situation development. It also describes how information is converted to intelligence to satisfy the commander's PIR. Analysis in support of situation development continues the IPB process and portrays significant aspects of the enemy, weather, and terrain in support of the decision-making process. This portrayal is baeed on the analysis of information from all sources that previously has been recorded, cataloged, and evaluated in a manner to facilitate effective analysis. This intelligence data base is continuously updated to ensure the information in it is current and accurate.

Automation increases the capability to manipulate large volumes of information from many sources and assist in the analysis process. However, analysis continues to be a human function. Information is interpreted by an analyst who adds the element of judgment, which is essential "to effective intelligence analysis.

History provides many examples of intelligence failures that are directly attributable to faulty analysis by people. In some cases, the indicators were present, but were either not recognized or were misinterpreted due to the analyst's preconceptions of the situation. In others, the analysis was correct, but was not presented in such a way that decision makers would accept it.

The primary product of intelligence analysis is the intelligence estimate. The estimate provides the best possible answer to the commander's PIR that is available at the time. The estimate is dynamic, constantly changing with the situation. Thus, analysis is conducted continuously with the information available. The available information almost always is incomplete. The analyst uses what is known about the enemy, weather, and terrain from the IPB to estimate what is not known. In addition, the analyst determines the enemy's capabilities, which are the basis for predicting probable courses of action.

ENEMY CAPABILITIES

Enemy capabilities are courses of action which the enemy can take to influence the accomplishment of the friendly mission. They indicate--

- What the enemy can do.

- When the enemy can do it.
- Where the enemy can do it.
- In what strength the enemy can do it.

The PIR normally are about enemy capabilities. Estimates of enemy capabilities and their probability of adoption impact significantly on the friendly commander's scheme of fire and maneuver for accomplishing the mission. By integrating the enemy's tactical doctrine, characteristics of the AO, and time and space factors as developed through IPB, the analyst estimates enemy capabilities with a reasonable degree of confidence. Enemy actions that would have little effect on friendly operations, would not benefit the enemy, or are not tactically feasible are not considered enemy capabilities. For example, an enemy force normally disengages its troops in an adjacent area to free these for commitment within our sector or zone. However, in some circumstances, this is not a viable enemy option. Therefore, in those circumstances this capability normally is not considered as an option.

Generally, there are four tactical courses of action open to the enemy in conventional operations: attack, defend, reinforce, or conduct a retrograde movement. These are divided into a variety of more specific courses of action. For example, an attack may be a penetration, an envelopment, or other variations of an attack. A retrograde movement may be a delaying action, a withdrawal, or a retirement.

Some enemy capabilities refer specifically to the support of combat forces rather than the capabilities of the combat forces themselves. Support capabilities include--

- Use of NBC weapons.
- EW.

Support capabilities always are considered, especially when enemy implementation of them will significantly affect the accomplishment of the friendly mission.

The analyst considers when the enemy can implement a capability. Time is a critical factor in the Air Land Battle; the friendly commander relies on time to defeat enemy first-echelon forces before follow-on echelon forces are committed to the battle. The friendly commander needs an accurate estimate of when enemy forces are employed to decide how to fight the battle. The analyst considers the following factors in estimating when an enemy force will be employed:

- Mobility capabilities.
- Disposition.
- Doctrinal rates of movement.

APPENDIX C

INDICATORS OF ENEMY COURSES OF ACTION

Indicators are any positive or negative evidence of enemy activity or any characteristic of the AO that points toward enemy capabilities, vulnerabil ities, or intentions. Individual indicators cannot stand alone. Each indicator is integrated with other factors and indicators before patterns are detected and enemy intentions established. Indicators are developed by the ASPS analysts who are assisted by other TOC elements in the G2 or S2 section. All indicators are developed to answer the commander's PIR and IR. The analyst uses indicators to correlate particular events or activities with probable enemy courses of action.

Indicators are also used to determine what events or activities occur for an enemy to follow a particular course of action. The ability to read indicators (including recognition of enemy deception indicators) contributes to the success of friendly operations.

Enemy deception operations provide indicators in an attempt to create false or misleading patterns of enemy intentions. Analysts detect these false indicators and then determine what actual courses of action the enemy is attempting to initiate. Enemy attempts at deception are discovered by comparing indicators, intelligence, and combat information from all sources to arrive at an accurate picture of the battlefield.

INTELLIGENCE INDICATORS

Tables C-1 through C-7 show different types of intelligence indicators. These lists of indicators are by no means complete, nor are they intended to apply to all situations or all types of enemy forces. They give some types of indicators which when incorporated with other indicators, creates patterns or suggests a series of activities which point to typical enemy activities or cour ses of action. Analysts are prepared to develop their own indicator ists for the specific situations which confront them.

TableC-l. Enemy offensive indicators.

ACTIVITY	EXPLANATION
Massing of motorized elements, tanks, artillery, and logistical support.	Areas of secondary importance are often denuded to mass maximum strength for the main effort.
Deployment of combat element (motorized rifle, armor, antitank (AT)) echelons on a relatively narrow frontage.	Normal attack formation provides for the second echelon of the regiment to be located 5-15 km in the rear of the first echelon, on-line; and the division second echelon 15-30 km in the rear of the first echelon.

Table C-1. Enemy offensive Indicators (continued).

ACTIVITY	EXPLANAT10N
Forward units disposed on relatively narrow fronts and depths.	A MRR breakthrough zone is from 2-4 km within an assigned attack frontage, which varies from 3-8 km. MRR headquarters located approximately 4 km from the FLOT during normal attack posture.
Concentration of mass toward e ther or both flanks within f rst echelon defensive area.	Single or double envelopment normally is attempted in the offense. Tanks and motorized units on either or both f anks may indicate single or double envelopment.
Demonstrations and feints.	Local, small-scale attacks or demonstrations involving motorized rifle units, tanks, and artillery frequently precede a general attack.
Establishment and strengthening counterreconna issance screen.	Counterreconnaissance screens are used to cover possible assembly areas, routes of troop movement, or regrouping of forces to be used in the attack.
Forward movement of hostile units.	Before launching an attack, troops may be moved to assembly areas from which they can deploy.
Increased patrolling (ground reconnaissance) .	Patrolling by motorized rifle units usually is more active before an attack.
Forward CPS located close to the FLOT. Other CPS move forward.	Preceding an attack, an auxiliary CP is establ ished, if needed, by Army or front. The division main CP is located 5-15 km from the FLOT; the division forward CP is located 5 km from the FLOT; the regiment main CP is located 2-3 km from the FLOT; and the battalion CP or OP is located 500-1,000 m from the F LOT.
Locating a division-sized operation maneuver group (OMG) at Army; Army-sized OMG at front.	OMGS are formed preceding an offensive operation. They are generally committed before the conclusion of the first echelon battle and operate independently of the main forces. OMGS use a separate axis of advance from the main body.

Table C-1. Enemy offensive Indicators (continued).

ACTIVITY	EXPLANAT 10N
Massing of artillery units.	Large RAGs, DAGs, and Army artillery groups (AAGs) indicate initiation of main attack. Enemy norms are 60-100 tubes per kilometer of frontage against wel l-prepared defenses for main attack; 60-80 tubes per kilometer of frontage against hasty defenses for main attack; and 40 tubes per kilometer frontage for secondary attack. The RAG is usually located 1-4 km from the FLOT; the DAG usually 3-6 km from the FLOT; and the AAG is usually more than 6 km from the FLOT. AAGs are formed only in the offense and only to support the main attack. TMS-65 are within 4 km of the FLOT for smoke operations.
Extensive artillery preparation of up to 50 minutes in duration.	The offense is built around the striking power and shock of massed artillery. Preparations of 1/2 to 1 hour normally precede an offensive.
Dispersal of tanks and self-propelled howitzers to units.	Tanks accompanying leading waves of assault motorized units--with motorized self-propelled howitzers following the tanks closely, by bounds.
Movement of fire and missile forward.	Enemy SAM control radars require time to be set up and oriented. The enemy prefers to establish SAM capability before moving other forces forward. In the event of the arrival of the second echelon, control radars are establ ished to allow for an overlap of coverage as the first echelon moves their SAM radars forward in the offense.
FROG, SS-21, SS-23, and SCUD units located forward.	Enemy offensive operations also occur in-depth. Forward movement of SSMS puts friendly airfields and depots in jeopardy.
2 to 4 ZSU-23-4S located in forward areas.	Medium AD guns are displaced before attack to protect assault forces and to facilitate forward displacement during the attack. ZSU 23-4s protecting the leading battalions are approximately 1.25 km to the rear of the FLOT.

Table C-1. Enemy offensive indicators (continued).

ACTIVITY	EXPLANAT 10N
Increased air reconnaissance,	Air reconnaissance usually is more active before an attack.
Systematic air bombardment.	Before the attack, the enemy may engage in the systematic "softening up" of key positions by bombardment,
Establishment of auxiliary airfields or activation of inactive air fields.	Buildup of logistics and maintenance capability indicates increased capability to support offense.
Clearing lanes through obstacles within own position.	Lanes are cleared and marked through mined areas, and ramps and bridges prepared over ditches and trenches within enemy's own position. This is done before attack to facilitate forward movement and grouping, particularly at night.
Reconnaissance and destruction of obstacles that are part of our defenses.	Usually on the night preceding an attack, enemy patrols reconnoiter friendly obstacles to determine a plan for clearing lanes. The patrol destroys only such obstacles that will not disclose the direction of the main attack.
River assault crossing units located forward (providing there is a water obstacle) .	Amphibious, bridge, and other engineer units with water-crossing capabilities are located near the FLOT and also echeloned to the rear. They are also collocated with other tactical units of the attacking force.
Airborne, airmobile, and air assault attacks on our rear area.	The enemy conducts offensive operations throughout the depth of the defense. Heliborne attacks are also made to facilitate difficult operations, like river crossings.
Increased enemy agent activity in rear area.	The enemy attempts to prevent or disrupt the forward movement of friendly supplies, equipment, maintenance, and reinforcements.
Extensive efforts to destroy nuclear storage areas and delivery systems by air, artillery, and sabotage.	Enemy doctrine calls for the elimination of friendly nuclear weapons by any means. The enemy considers that we are more likely to use nuclear weapons when we are in the defense.

Table C-1. Enemy offensive indicators (continua).

ACTIVITY	EXPLANAT 10N
Movement of noncombatants out of the combat zone.	Noncombatants hinder rapid forward movement of follow-on forces.
Conducting drills and rehearsals in rear areas.	Major attacks may be preceded by drills or rehearsals. This is particularly true of attacks against fortified positions or strongly defended river lines.
Increased activity in rear areas.	Before an attack, supply and administrative activities increase in the rear areas.
Traffic control units marking routes to the FLOT.	Traffic control points are employed throughout the march routes to facilitate march formations. Allied border guards assist by controlling traffic through the barrier areas of the borders.
Forward placement of supply and evacuation installations.	Supply and evacuation installations usually are located well forward for an attack, Technical observation points are established close to the FLOT. Repair and evacuation groups are located at assembly points close to the FLOT to repair or evacuate damaged vehicles. The division supply point (ammunition, petroleum, oil, and lubricants (POL), rations) is located 25-30 km from FLOT. The regimental amrnunition supply point is located 10-15 km from the FLOT; the regimental repair point is located 10-15 km from the FLOT; the regimental POL point is located 10-15 km from the FLOT, and the regimental rations point is located 10-15 km from the FLOT. Battalion ammunition and rations supply points are located 5 km from the FLOT. The division repair point for tanks and weapons is located 2-4 km from the FLOT. The division repair point for wheeled vehicles is located 10-14 km from the FLOT. Rear control points for the front are located 150-200 km from the FLOT; for the Army are 25-40 km from the FLOT; for the division is 20 km from the FLOT; and for the regiment are 20 km from the FLOT.

Table C-1. Enemy offensive indicators (continued).

ACTIVITY	EXPLANAT 10N
Location of maintenance parties on lateral routes.	When the enemy conducts a march, the enemy establishes several maintenance parties on lateral routes to facilitate march operations.
Medical points and stations move forward.	Medical units move forward before an offensive operation to support anticipated medical and evacuation requirements. Division medical points and stations are located 10-14 km from the FLOT; the regimental medical points and station at 10-14 km from the FLOT; and the battalion medical points and station at 1.5-3 km from the FLOT.
Radio sil ence on nets organ c to the d vision.	The enemy attempts to deny us information which can be developed from intercepting radio traffic.
Abnormal logistics traffic on command nets.	To expedite supplies to units about to conduct a main attack, commanders may get personally involved.
Dummy traffic in radio nets to cover unit moves.	The enemy will attempt to deceive us about the location of enemy forces.
Deception operations to cover unit movement.	Same as above.
Extensive smoke operations.	Smoke operations mask the movement of units during the period immediately preceding an attack.
SIGINT and jamming assets located forward.	SIGINT and jamming assets will move well forward to within 2-4 km of the FEBA before attack.
Extensive spot and barrage jamming of our front line units' communications nets, as well as communications systems associated with tactical air control systems.	Extensive jamming will precede an offense to cause the maximum disruption of our C^2 communications. However, jamming will cease when enemy forces reach our main defense area to prevent interference with their own communications systems.

Table C-2. Enemy defensive indicators.

ACTIVITY	EXPLANAT 10N
Preparation of battalion and company defense areas consisting of company and platoon strong points.	Defense is based on holding prepared defensive areas and counterattacks by tank-heavy forces.
Extensive preparation of field fortifications.	The enemy makes extensive use of trenches, prepared positions, and overhead cover in defensive operations.
Formation of AT strongpoints in depth along avenues of logical approach.	AT strongpoints are formed in depth along logical avenues of approach for armor. These are made up of motorized rifle, engineer, and AT gun and missile units with positions strengthened by mines, ditches, and other obstac es.
Attachment of additional AT units to frontline defensive positions.	In areas where there is a serious armored threat, the enemy will concentrate as many as 25 AT guns for every 1,000 m of front.
Preparation of alternate artillery positions.	In normal defensive operations, three positions are prepared for each firing battery.
Employment of roving artillery.	Roving guns and batteries are part of normal defensive operations.
Large tank heavy units located in assembly areas to the rear.	Tank units are held in assembly areas for employment in counterattacks.
Preparation and occupation of defensive positions.	In the defense, a security zone and main defense area are prepared and occupied.
Presence of demolitions, contaminated areas, obstacl es, minefield.	Demolitions, minefield, and other obstacles are placed to cover AA to the position.
Deployment of motorized rif e units on good defensive POSi tions. Preparation of company strongpoints on key terrain	Dominating terrain that has good FofFs and is relatively inaccessible to tanks usually is selected for a defensive position.

Table C-2. Enemy defensive indicators (continued).

ACTIVITY	EXPLANATION
Prestocking ammunition and engineer supplies and equipment and fortification of buildings.	Prestocking ammunition reduces the load on logistics throughout the system once the battle begins, Engineer tools and equipment may be used to dig trenches and to erect obstacles.
Entrenching and erecting bands of wire.	Digging of trenches and the erection of wire indicate preparations to hold the position.
Presence of dummy artillery observation points.	Dummy artillery observation points preserve the effectiveness of the actual artillery positions by deceiving us as to their location.
Presence of dummy CPS.	Same as above.
Increased activity of SIGINT and ESM units but decreased activity of ECM units.	Increased activity is an attempt to gain information about us before the attack.
Early warning sites hardened.	When early warning sites are hardened, it indicates the intention of those forces to remain in place and to protect an important facility.
CPS placed in hardened facili ty.	Same as above.
Additional AT units attached to first eche on maneuver uni ts.	The enemy puts great emphasis on killing tanks early. The enemy believes that if the tanks can be stopped, the attack will fail.
Establishment of a security zone.	A security zone is established to enable fortifications to be constructed away from immediate danger from our artillery and direct-fire weapons.
Forward units disposed on relatively wide fronts and depths compared to offensive posture.	The defense zone of an MRR varies from 10 to 15 km depending upon terrain and the combat availability of forces. MRR depth varies from 7 to 10 km.

Table C-2. Enemy defensive indicators (continued).

ACTIVITY	EXPLANATION
Displacement of logistics and units towards the rear.	Logistics and medical units are displaced to the rear to facilitate combat force defense and counterattack operations.
Displacement of artillery and SSM units towards the rear,	Artillery units are displaced toward the rear to reduce the chance that these units will be lost or destroyed during the preliminary stages of the battle. During the defense, deep fires are not as critical as during the offense.
Presence of large AT reserves with mobile obstacle detachments (MODS).	Large AT reserves are established (with MOD) to provide a quick reaction AT capability.
Decreased communications intercepts (due to increased use of wire).	The enemy places increased reliance on wire in the defense to increase security.
AD systems located in rear areas.	Destruction of logistics, command, and artillery units are high-priority missions for our deep attacks,

Table C-3. Meeting engagement (movement to contact) indicators.

INDICATORS

ACTIVITY	EXPLANATION
Increased air and ground reconnaissance along MCS.	Accurate information about routes speeds the advance.
Road junctions, bridges, and other key features are occupied by either airborne forces or forward detachments.	The enemy wants to control high-speed armor AAs into our key areas.
Increased counterreconnaissance activity.	Counterreconnaissance is an attempt to prevent us from gaining information about enemy dispositions and movements.
Forward movement of columns dispersed laterally in two or more MCS.	The enemy prefers to use march formation when moving to contact.

Table C-4. Reinforcement indicators.

ACTIVITY	EXPLANATION
Movement of additional troops toward the front.	This action increases enemy's present strength.
Increased traffic toward present position.	Increased traffic brings up additional troops, equipment, and supplies.
Identification of new units in in the combat zone.	The presence of new units--in addition to units already present--increases enemy's strength.
Additional CPS and supply and evacuation installations.	Presence of additional units causes an increase in the number of these installations.
Logistical installations moved well forward.	indicates preparation for the resumption of the offensive after reinforcement.

Table C-5. Delaying action indicators.

ACTIVITY	EXPLANATION
Withdrawal from defensive position(s) before becoming heavily engaged.	In delaying actions, units avoid becoming decisively engaged.
Successive local counterattacks with limited objectives.	Counterattacks are employed o assist in disengaging first echelon units, rather than to restore posit on.
Counterattacks broken off before position is restored.	Same as above.
Maximum firepower positioned forward; firing initiated at long ranges.	Long-range fires facilitate the delaying action.
Frontages up to four times that normally assigned to units on the defensive.	Forces conducting a delaying action are normally assigned frontages in excess of that normal for enemy units on the defense.
Prepositioni ng of nuclear weapons.	Prepositioning nuclear weapons facilitates the delaying action.
Discovery of dummy minefield.	Dummy minefield are easier and faster to prepare than active fields but cause approximately the same delay to advancing pursuers.

Table C-6. Withdrawal indicators.

Indications for withdrawal are generally the same as those for delaying action with the addition of the following indicators,

ACTIVITY	EXPLANATION
Systematic destruction of bridges, communication facilities and other assets in enemy-held territory.	Deliberate demolition and scorched earth tactics may be employed in military withdrawals.
Establishment of a covering force and rear guard.	Cover movement or withdrawal of main body. The rear guard fights delaying action, if required,
Increased use of night-driving devices in all areas.	The enemy will attempt to withdraw at night, if possible.
Minimum logistical and medical services.	Nonessential logistics and medical services are withdrawn first.
Marking withdrawal routes.	Movement and location of traffic control units or parties to the rear along the LOCS that are to be used by major units.
Use of contaminated areas to camouflage forces and cover withdrawal .	Contamination hinders reconnaissance and pursuit.
Presence of rear guard and covering force.	Minimizes losses and permits main body more freedom of movement.
Preparation of future defensive lines behind main defensive structure.	If the withdrawal is deliberate, the enemy will want new positions ready before withdrawing.
Jamming or destruction of friendly air and ground battlefield surveillance radars.	Battlefield surveillance radars are capable of detecting withdrawals at night or during conditions of poor visibility.
Engineer reconnaissance and MOD detected along LOCs, tunnels, built-up areas, dams, and dikes.	Withdrawing forces will begin to systematically destroy all crossings and implement obstacles as they withdraw.

Table C-6. Withdrawal Indicators (continued).

ACTIVITY	EXPLANAT 10N
Stockpiling of explosives at central points. Distribution of, and the establishment of, small dumps of explosives and landmines near bridges, possible abatis sites, and other demolition target sites.	Wit hdrawing forces will attempt to de ay pursuit with obstacles,
Preparation of target for systematic or hasty destruction.	Same as above.
Deception operations, such as dummy radio traffic.	Withdrawing units will attempt to portray a normal defense.
Smoke operations to cover withdrawal operations.	Withdrawals must be unobserved to be effective.
Rearward movement of long-range artillery.	Long-range artillery will be moved back to new positions before the withdrawal takes place
Movement of small reconnai ssance parties to the rear.	Withdrawing units need current reconnaissance along w thdrawa routes.
Displacement to the rear of emitters associated with logistics units. Destruction or removal of logistic material from existing depot and dump locations to the rear.	Logistics are withdrawn first to avoid being overrun during a possible pursuit.

Table C-7. Nuclear weapons indicators.

ACTIVITY	EXPLANAT 10N
Heavily guarded movement of supplies, equipment, and material .	Movement of supplies, equipment, and material of nuclear nature requires special security measures.
Heavily guarded installations.	Sites for storage of nuclear supplies and the locations of del ivery units are heavily guarded.
Preparation of heavy artillery positions.	Primary and alternate positions for nuclear del ivery artillery are prepared before movement of the units.
Movement of small, heavily guarded convoys, including closed vans, with a high percentage of automatic weapons.	Nuclear warheads are moved under heavy security, usually in closed vans. Escort vehicles are equipped with machine guns.
Light aircraft circling over moving convoy.	Nuclear warhead convoys often use aerial radio relays to maintain communication.
Movement of small groups of heavily armed hel icopters escorted by tact cat fighters.	Nuclear warheads may be moved by helicopters, with guards and armed helicopters as escort, Tactical aircraft may provide air cover.
Movement of trai ers with rockets or missile bodies.	Trailers are used to resupply missile and rocket units.
Identification of tall, slender objects, like towers, chimneys, or narrow trees, not previously in the area.	Ballistic missiles may be camouflaged as towers, chimneys, or narrow trees, such as poplars.
Large, well-guarded complexes, including tanks, trucks, radars, electronic equipment, generators, and maintenance tents, located wel l to the rear.	SSM units require extensive ground handling equipment.
Evacuation or exclusion of civilians from specific areas suitable for nuclear storage or delivery sites.	Civilians may be evacuated from areas selected for nuclear storage or delivery sites.

Table C-7. Nuclear weapons indicators (continued).

ACTIVITY	EXPLANAT 10N
Presence of meteorological radars.	An END TRAY radar is part of the organic equipment of both the free rocket over ground (FROG) and SS-1c SCUD systems, as wel 1 as other nuclear-capable systems. (END TRAYS also are found with conventional artillery and AF units.)
Construction of FROG, SCUD, or SCALEBOARD, SS-21 or SS-23 launch positions.	All of these systems have confirmed nuclear capabilities. A survey-controlled launch position is constructed for each transporter-erector-launcher (TEL) before occupation.
Movement of SSM TELs to a launch site within 1/3 to 1/2 maximum range from the FLOT.	SSM TELs remain in camouflaged positions until movement to the launch area.
Passage of wind data from mid-range position to a command or technical element.	Enemy SSM accuracy is heavily dependent on wind data.
Passage of a nonsense word over command and selected fire control nets.	May be a code word relative to preparation for or execution of a nuclear fire mission.
Volume of traffic on command nets suddenly increasing then dropping to a low level or standdown.	May reflect passage of strike warnings followed by preparation for electro-magnetic pulse protective measures.
Identification of SSM unit-peculiar equipment.	Presence of nuclear-capable systems.
Limited withdrawal of frontline units without apparent tactical reason.	Frontline units may withdraw for a limited distance to avoid casualties from close-in nuclear explosives.
Sudden and energetic digging in enemy areas.	Prior to use of nuclear weapons, frontline units may be ordered to dig deeper foxholes or take other individual protective measures.

Table C-7. Nuclear weapons indicators (continued).

ACTIVITY	EXPLANAT 10N
Large concentrations of radios, radars, and other electronic equipment located in the vicinity of suitable sites for guided missile launching.	Concentration of equipment is necessary to guide and control guided missiles, which must be located in close proximity of the launching site.
Sudden increase in communications and electronic activity.	Increase may be incident to delivery of nuclear weapons, for example, last minute orders and warnings, and use of electronic guidance and control.
Use of smoke cover on front-line troops.	Smoke may be used to protect troops against thermal effects of weapons used in close support.
Disappearance of known enemy agents from specific areas.	Prior to nuclear attack of an area, agents may be ordered to leave the area.
Increased or unusual air activity.	Delivery of nuclear weapons by air may require a temporary degree of total air superiority, special photo mission, or practice flight pattern runs by the delivery aircraft.
Additional AT elements with first echelon units.	Enemy will expect friendly forces to react to indications of a nuclear strike with an attack of tank-heavy forces. Also, tanks have greater survivability under nuclear conditions.
Movement of small convoys from the warhead storage areas.	Warheads being moved to be mated to missiles.
Removal of antennas and other equipment mounted on the exterior of vehicles.	To prevent blast damage.
Lowering of windshields on vehicles.	See above.
Removal of camouflage nets.	See above.
Movement of vehicles to reverse slopes.	See above.

Table C-7. Nuclear weapons indicators (continued).

ACTIVITY	EXPLANAT 10N
Location of missile and free rocket units within striking distances.	Missile and free rocket units are located within one third of the maximum range from the I ine of contact on the offense, and one half of the maximum range on the defense.
Use of missiles or rockets with high-explosive warheads.	Missiles or free rockets may be used to deliver high-explosive warheads either in a normal support role or in a registration.
Location of very heavy artillery within supporting distance of front lines.	Nuclear delivery artillery is located within one third of its maximum range from the line of contract on the offense, and one half of the maximum range on the defense.
Registration of very heavy artillery.	Registration may be conducted using smoke and low charge or high explosive projectiles prior to firing a nuclear projectile.
Special or unusual activity by frontline troops.	Frontline troops may construct special positions, usually deep or covered foxholes, before enemy use of nuclear weapons.
AD weapons are deployed to cover possible warhead storage areas.	Enemy expects friendly air to attempt to destroy nuclear warheads in storage.
Use of high-explosive warheads from SSMs-or heavy art illery in a normal support role.	Indicates presence of nuclear-capable systems.
Use of missile-associat ed terms on selected radio nets	See above.
Preparation of future launching positions.	See above.
Inability to locate previous γ identified missile units.	May be moving to f iring positions.
Additional administrative, command, fire control, and logistics nets identified in the area of interest.	If these nets can be identified as nuclear-related, they indicate the presence of nuclear-capable units.

Table C-7. Nuclear weapons Indicator (continued).

ACTIVITY	EXPLANATION
Presence of heavy artillery,	203 mm SP gun, 240 mm SP mortar, and towed 203 and 240 have nuclear delivery capabilities, as do 152 mm SP guns.
Deployment of jamming assets.	Jammers are deployed to protect critical targets like nuclear units.

INSURGENT ACTIVITY INDICATORS

Anything that insurgents do to influence and direct a society toward overthrowing its government is reflected by some action or indication, no matter how subtle. These occurrences are referred to as insurgent activity indicators. By recognizing these indicators, it is possible to obtain the first clues to insurgent existence and then evidence of the growth of the insurgent movement. Because there is a great deal of legitimate activity, there is a requirement to determine which of the various sociological, economical, political, and other activities represent insurgent activity.

It is not possible to provide an all-inclusive listing of insurgency indicators because there are too many possibilities existing in the many nations of the world. The following indicators, however, do provide a beginning framework for a detailed analysis of any particular country. The greater the perception of an insurgency situation within a particular country and the greater the knowledge of the insurgent involved, the easier it is to identify the insurgent activity indicators.

These indicators serve as a guide for intelligence officers and analysts in developing appropriate clues to insurgent activity in a particular area. Isolated actions of seemingly little significance in one area show a pattern of an emerging insurgency when coordinated with reports of indicators from other areas. In developing indicators, or using these suggested ones, it is important to remember that insurgent strategy suddenly changes. The insurgent threat unfolds along altogether different lines simultaneously or suddenly switches from use of military force, for example, to a political example, to a political offensive. Such a development is dangerous if it makes the general situation appear to be much less critical than it" really is. The development of appropriate indicators not only indicates that an insurgency or potential insurgent situation exists, but also identifies any problems and dissatisfaction of the people. The elimination or effective control of insurgency is based on coordinated internal defense and development (IDAD) programs which address identified problems or potential problems. Before these programs are developed, the threat is defined. To define the threat, you first establish insurgent activity indicators.

RURAL INSURGENT ACTIVITY

A rural area includes all farming areas, any town or village up to 5,000 people, and any town or village up to 20,000 people with a farm-based economy where the townspeople, if not engaged in farming, earn their livelihood in agricultural service industries. In such areas, where the interests are so interdependent, insurgency indicators would be similar in both the town and countryside. This is not to say that rural insurgency is not directed by urban insurgents and coordinated with urban insurgency; however, some theorists emphasize that the key to success is the countryside and the rural population. In such cases, early insurgency indicaters are found in the rural areas where the subversive insurgents are concentrating their initial efforts.

During the development of a subversive insurgency, some of the first indicators of latent or incipient insurgency appear in the rural areas. While some of these indicators are rather obvious, some are not. For the sake of simplicity, these indicators of insurgency are placed into four categories: population, propaganda, commodity, and environmental.

Population

Population indicators are broken down further into subcategories of general activity, insurgent-promoted activity, and activity directed against the government.

General Activity. This includes--

- Identification of insurgents, their supporters, and sympathizers who suddenly appear in, or move out of, an area.
- New faces in the community.
- Unusual gatherings among the population.
- Disruption of normal social patterns.

Insurgent-Promoted Activities. This includes--

- Refusal of peasants to pay rent, taxes, or loan payments or unusual difficulty in the collection of same.
- Trends of demonstrated hosti l ity on the part of the local population toward government forces.
- Occurrence of actions previously considered taboo by the POPUlace.
- Disappearance of the population from or avoidance by the peeple of certain areas.
- Unexplained disappearance or dislocation of young people.

Activity Directed Against the Government. This includes--

- Strangers attempting to join local security forces.
- Reports of the people being approached for purposes of intelligence recruitment.
- Unusual short absences of government employees.
- Failure of police and informant nets to report properly.
- Growth of general hostility toward the government.

- Unexplained destruction *or* loss of government identification papers or passports and increased forgeries thereof,

- Closing of rural schools.

- Murder and kidnapping of local government officials.

Propaganda

Propaganda indicators are broken down further into subcategories of general activity and activity directed against the established government, national military forces, and the educational system:

General Propaganda Indicators. This includes--

- Dissident propaganda from unidentified sources.

- Increase in the number of entertainers with a political message.

- Increasing religious unrest.

- Increased agitation on issues for which there is no identified movement or organization.

- Renewed activity by insurgent organizations thought to be dormant.

- Circulation of petitions advocating usual insurgent demands.

- Reports from other countries that the country is ready for revolution.

Directed Against the Established Government. This includes--

- Attempts to discredit and ridicule national or public officials.

- Attempts to discredit the judicial system and POI ice organizations.

- Characterization of government leaders as puppets and tools of a foreign government.

- Movement to remove strong anti insurgency leaders.

- Agitation against government projects and plans.

- Rumors designed to gain public acceptance of untruths about the government or governmental leaders.

- Advocacy of popular front government.

Directed Against the National Military Forces. This includes--

- Attacks which embarrass or ridicule military officials.
- Characterization of military leaders as puppets and tools of a foreign government.
- Movement to remove strong anti insurgency leaders from the military.
- Propaganda directed toward youth to refrain them from joining the military service or propaganda directed at soldiers to desert.
- Characterization of the armed forces as the enemy of the people.
- Civilian avoidance of and reluctance to cooperate with the military.

Directed Against the Educational System. This includes--

- Appearance of questionable doctrine in the educational system.
- Charges by students and others that the educational system is not adequate and is only training the youth of the nation to do the government's bidding.

Commodity

Commodity indicators are broken down further into crops, animals, arms and ammunition, clothing, drugs and medicine, and communication activity subcategories.

Crops. This includes--

- Diversion of crops from the market.
- Unexplained decrease in the marketing of a given crop.
- Increased reports of pilfering foodstuffs.
- Strangers attempting to purchase crops or produce.
- Farmers marketing a crop that is smaller than usual, yet showing no signs of subsequent financial difficulty.
- Discovery of caches of staple foodstuffs.
- Increase in crop prices indicating the existence of an insurgent taxing authority in the area.

Animals. This includes--

- Diversion of animals or meat from the market.

- Reports of loss of hides or diversion of hides from the market.

- Disappearance of wild game from an area in which it was previously plentiful.

- Disappearance of pack animals or the appearance of unusual numbers of pack animals in certain areas.

Arms and Ammunition. This includes--

- increased loss of weapons by military and police forces.

- Increased thefts of weapons.

- Discovery of arms caches.

- Attacks on patrols resulting in loss of weapons and ammunition.

The above factors could be applied not only to weapons but also to any similarly essential military goods.

Clothing. This includes--

- Unusual scarcity of any type of material that could be used for footwear. This could include such items as hides of animals and old tires, in addition to manufactured footwear.

- Discovery of caches of clothing or of materials which may be used in the manufacture of clothing or uniforms.

Drugs and Medicine. This includes--

- Scarcity of herbs and plants used in or for drugs and medicine.

- Large-scale purchasing or theft of drugs and medicine and of the herbs used in their manufacture.

Communications. This includes--

- increases in purchase and use of radios.

- Discovery of caches of communications equipment.

- Unusual increase in communications traffic in amateur radio operations.

Environmental

The environmental indicators include--

- Evidence of increased foot traffic in the area.

- Increased travel within and into remote or isolated areas.

- Unexplained trails and cold campsites.

- Establishment of new, unexplained agricultural areas, or recently cleared fields.

- Unusual smoke, possibly indicating the presence of a campsite or a form of communication.

- Concentration of dead foliage in an area, possibly indicating use of camouflage.

- Presence of foot traps, spikes, and the like.

- Presence of obstacles such as those used in roadblocks and canal blocks.

URBAN INSURGENT ACTIVITY

Indicaters of urban insurgent activity also are placed in the four categories of population, propaganda, commodity, and environmental indicators. Many of the same or similar indicators appear for both rural and urban areas.

Population

Population indicators are broken down further into subcategories of general activity, insurgent-promoted activity, and activity directed against the government.

General Activity. This includes--

- Increase in size of embassy or consulate staffs from a country or countries which support insurgent groups.

- Increase in staff and activities in pro insurgency-oriented embassies or consulates in neighboring countries, including unusual patterns in nature and volume of external communications (both in-country and out-of-country).

- Increased travel by suspected subversives to pro insurgency-oriented countries or to countries notably under insurgent influence.

- Influx of insurgent leaders, both foreign and domestic, into the urban area.

- Reports of locals being trained in pro insurgency-oriented countries.

- Increase in visitors from pro insurgency-oriented countries (tourists, technicians, businessmen, and officials).

- Close connections between the diplomatic representatives of pro insurgency-oriented countries and the insurgents.

- Disappearance of known or suspected insurgents and dissident elements.

- Increase in insurgent youth gatherings.

- Hosting of trade fairs or similar activities by pro insurgency-oriented countries.

- Return of nationals from travel or study in pro insurgency-oriented countries.

- Increase in visits to urban centers by rural officials and leaders from areas of unrest.

- Establishment of organizations (even very small) of unexplained origin and of unclear or nebulous aims.

- Establishment of a new organization to replace an existing organizational structure with identical aims.

- Appearance of many new members in established organizations like labor unions,

- Attempts by new groups to obtain control of established organizations.

- Infiltration of student organizations and unions by known agitators.

- Appearance of new organizations with titles stressing patriotism, grievances, or interests of underprivileged or minority groups.

- Reports of large donations to new or revamped organizations.

- Reports of payments to locals for engaging in subversive activities.

- Reports of the formation of subversive paramilitary organizations.

- Use of grenades or other explosives in terrorist acts.

- Reports of insurgent lists of targets for planned terroristic acts.

- Appearance of professional agitators in demonstrations that result in violence.

- Evidence of the participation of paid and armed demonstrators in riots.

Insurgent-Promoted Activities. This includes--

- Reported incidents of attempted recruitment of people to join new movements or underground organizations.
- Unexplained unavailability or disappearance of doctors, printers, and other specialists who may be working with and for the insurgents.
- Habitual criminals and unruly youths who seem to be acting with and for the insurgents.
- Increased unrest and agitation among laborers.
- Inability or refusal of people to pay taxes.
- Reports of extortion and other coercion by the insurgents to obtain financial "donations" from the people.
- Disappearance of young men from the city.

Activity Directed Against the Government. This includes--

- Failure of police and informant nets to report properly, indicating sources are supporting the insurgents or are afraid of them.
- Decreasing success of government agents in infiltrating subversive organizations.
- Assessination or disappearance of government agents.
- Reports of increased attempts by insurgent representatives or suspected subversives to make contact with local leaders or government officials.
- Reports of attempts to bribe or blackmail government and law enforcement employees.
- Reports of attempts to get classified information from government officials or documents from government offices.
- Leakage of classified information to news media.
- Sudden improvement in financial status of certain government and law enforcement employees.
- Failure of government raids on suspected subversive meetings or headquarters apparently because of forewarning.
- Increased activity against the government and its police, minority groups, foreigners, or similar groups.

- Demonstrations against government forces, scapegoat minority groups, or foreigners, designed to goad government forces into acting against crowds.

- More articles or advertisements in newspapers criticizing the government.

- Growth of general hostility toward the government and law enforcement agencies.

- Occurrence of strikes in critical areas casting doubt upon the ability of the government to maintain order and provide for the needs of the people.

- Unusual and unsatisfactorily explained absences of government employees from their offices.

- Sporadic, unexplained destruction, loss, or forgery of government identification cards and passports.

- Unexplained disruptions of public utilities.

- Reports of extortion attempts on local leaders and businessmen.

- Terrorist acts and threats against government and business leaders.

- Murder or kidnapping of government officials.

Propaganda

Propaganda categories are broken down further into categories of general activity, and activity directed against the established government, military and police, and educational systems.

General Activity. This includes--

- Worldwide propaganda by proinsurgency-oriented countries denouncing conditions and blaming the government of the targeted country.

- Appearance in-country of antigovernment slogans and pronouncements by word of mouth, wall scribbling, posters, and leaflets.

- Letter writing campaigns to newspapers and government officials deploring undesirable conditions and blaming individuals in power.

- Increased use of slogans pinpointing specific grievances.

- Increased use of petitions demanding government redress of grievances.

- Circulation of petitions and pamphlets which appear to follow the beliefs and policies of a foreign power.

- More rumors, publications, or leaders from areas occupied by migrants which focus upon lack of official concern about poor conditions.

- More agitation and unrest within the urban population for which there is no logical explanation,

- Appearance of committees and organizations whose leaders do not seem to be from the urban area, yet who purport to speak for the citizens of that area.

- increased appeals directed at intensifying general religious unrest in countries where reiigious competition exists.

- Mass demonstrations where participants voice standard Communist demands.

- Announcements by foreign countries that the concerned country is ripe for "war of national iiteration, " or words to that effect,

- Propaganda linking local ethnic groups with those in neighboring countries.

- Clandestine in-country radio broadcasts worded to appeai to those with special grievances or to underprivileged ethnic groups.

- Use of bullhorns, truck-mounted loudspeakers, and other sophisticated equipment in "spontaneous"' demonstrations.

- Presence of photographers other than newsmen among demonstrators.

- Widespread propaganda which appeals for sympathetic reception or participation in strikes or demonstrations.

- Rallies to honor "martyred" insurgents. Mass demonstrations honoring revolutionary heroes or dates significant to insurgency.

- Nationwide strikes tailed to demonstrate the strength of the insurgent movement.

- Sympathy strikes or demonstrations taking place outside the country concerned.

Activity Directed Against the Established Government. This includes--

- Radio propaganda from foreign countries, aimed at the target country, accusing its government of failure to meet the needs and desires of its people.

- Propaganda from foreign countries, aimed at the target country, denouncing imperialism.

- Demonstrations and violence in foreign countries against embassies, offices, and consulates of the target country or countries which support its government.

- Spreading accusations that the government is corrupt and completely out of touch with the people.

- Agitation against existing or proposed government projects and plans.

- Accusations that the government is a pawn of a foreign government.

- Calls for a popular front government, including new parties.

- Character assassinations of top government officials.

- Movement to remove strong anti insurgency leaders from office.

- Strikes or work stoppages called to protect government actions.

Activity Directed Against the Military and Police. This includes--

- Spreading accusations that the military and police are corrupt and completely out of touch with the people.

- Character assassinations of military and police officials.

- Movement to remove strong anti insurgency military and police leaders from the office.

- Calling on the people to stop cooperating with the military and police.

- Deliberate acts to provoke police reprisals during demonstrations or strikes.

- Accusations of police brutality or ineffectiveness or claims that government forces initiated violence when demonstrations end in riots.

- Publication of photographs purporting to show repressive police practices.

Activity Directed Against the Educational System. This includes--

- Student unrest manifested by new organizations, proclamations, demonstrations, and strikes against authority.

- Charges by students and others that the educational system is not adequate and is only training youth to do the government's bidding.

- Appearance of questionable doctrine in the educational system.

- Clamor for personnel changes in the educational system.

Commodity

Commodity indicators are broken down further into subcategories of foods, arms and ammunition, clothing, and drugs.

Foods. This includes--

- Scarce food supplies when there is no report of natural impediments to agriculture.

- Decline of foodstuffs in a country or province where there is a tolerated black market, which indicates that the food is being diverted.

- Sudden shortages of preserved foods or items of food requiring minimal storage facilities.

- Failure of farmers to transport their products to the city, indicating a fear of travel on the highways.

- Large-scale purchasing of foodstuffs which may be by purchasing agents for an insurgent movement.

Arms and Ammunition. This includes--

- Increase in assaults on police and military personnel which results in thefts of weapons.

- Increase in thefts and purchases of arms, ammunition, and explosives.

- Discovery of arms, ammunition, and explosives being clandestinely manufactured, transported, or cached.

- Increased purchase and theft from salvage yards of metal products like pipe, casings, wire, spikes, snd nails.

- Increased purchase of surplus military goods.

- Increase in demand for small arms and ammunition on the open market.

- Reports of large-scale purchasing of weapons, ammunition, and material used in their manufacture.

- Increase in pilfering of arms and ammunition from the government.

- Increase in the number of armed robberies.

- Reports of theft or sudden shortages of chemicals which could be used in the clandestine manufacture of explosives.

- Appearance of arms manufactured in pro insurgency-oriented countries.

Clothing. This includes--

- Unusual systematic purchase of clothing materials which could be used for the manufacture of insurgent uniforms or footwear.

- Unusual scarcity of clothing or material used in the manufacture of clothing and footwear.

- Distribution of clothing to underprivileged classes by organizations of recent or suspect origin.

- Discovery of caches of uniform clothing.

Drugs. This includes--

- Scarcity of drugs and medical supplies on the market or black market.

- Large-scale purchase or theft of drugs and other medical supplies,

- Diversion of shipments of drugs.

Environmental

The environmental indicators include--

- Apartments and housing being rented, but not lived in as homes.

- Slogans written on walls, bridges, and streets.

- Defacement of government and police information signs.

- Disappearance of electrical lines. Pollution of the urban area's water supply.

- Terror ist acts against physical targets like bridges, dams, airports, or buildings.

- Changes in residence of suspected subversives.

- Discovery of message drops.

- Apartments and houses being used for purchases other than residences.

- Increased smuggling of currency, gold, gems, narcotics, medical supplies, and arms into urban centers.

- Reports that local currency is being bought up in world markets by pro insurgency-oriented countries.
- Appearance of abnormal amounts of counterfeit currency.
- Increase in bank robberies.
- Work stoppages or slowdowns in essential industries.
- Marked decline in product quality in essential industries.
- Marked increases in equipment failures in essential industries.
- Mass strikes and sympathy strikes in essential industries.
- Appearance of known agitators or suspected subversives in picket lines.
- Escalation of peaceful strikes to violence against property and nonstriking personnel.
- Explosions in essential utilities and industries,
- Roadblocks and mines on main lines of communication.
- Malicious damage to industrial products or factory machinery.

FIELD MANUAL
NO. 34-60

*FM 34-60
HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 3 October 1995

COUNTERINTELLIGENCE

TABLE OF CONTENTS

Page

PREFACE iii

CHAPTER 1 – MISSION AND STRUCTURE 1-1
General 1-1
Mission 1-2
CI in Support of Force XXI 1-4
Intelligence Tasks 1-6
CI Tasks 1-6
Army CI as a Function of MI 1-7
Counterreconnaissance 1-7
Other Specialties 1-7
Peace, War, and OOTW 1-8
The CI Structure 1-9
CI Support to US Forces 1-11
Planning 1-12
Tasking and Reporting 1-12
Joint and Combined Operations 1-13
Legal Review 1-15

CHAPTER 2 – INVESTIGATIONS 2-1
General 2-1
Types of Investigations 2-1

CHAPTER 3 – OPERATIONS AND TECHNIQUES 3-1
General 3-1
Operations 3-1
Techniques 3-14

CHAPTER 4 – COUNTERINTELLIGENCE COLLECTION ACTIVITIES 4-1
General 4-1

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes FM 34-60, 5 February 1990.

Section V

PERSONALITIES, ORGANIZATIONS, AND INSTALLATIONS LIST

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-V-1. **GeneraI.** The effectiveness of CI operations depends largely on the planning that precedes the operation. Early in the planning process the CI officer on the G2 staff directs the efforts to obtain information on the adversary's intelligence, sabotage, terrorism, and subversion capabilities. Collected information is processed and analyzed, and from it the CI officer formulates a list of CI targets. Section V identifies the criteria for the personalities, organizations, and installations list. CI targets are personalities, organizations, and installations of intelligence or CI interest which must be seized, exploited, or protected.

A-V-2. **Personalities.** These are persons who are a threat to security, whose intentions are unknown, or who can assist the intelligence and CI efforts of the command. Personalities are grouped into these three categories. For ease in identification, a color code indicates the category. Colors currently in use are black, gray, and white and pertain to the three categories in the order listed above.

a. Black list. The black list is an official CI listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of the friendly forces. (Joint Pub 1-02) Black list includes—

(1) Known or suspected enemy or hostile espionage agents, saboteurs, terrorists, political figures, and subversive individuals.

(2) Known or suspected leaders and members of hostile paramilitary, partisan, or guerrilla groups.

(3) Political leaders known or suspected to be hostile to the military and political objectives of the US or an allied nation.

(4) Known or suspected officials of enemy governments whose presence in the theater of operations poses a security threat to the US Forces.

(5) Known or suspected enemy collaborators and sympathizers whose presence in the theater of operations poses a security threat to the US Forces.

(6) Known enemy military or civilian personnel who have engaged in intelligence, CI, security, police, or political indoctrination activities among troops or civilians.

(7) Other personalities indicated by the G2 as automatic arrestees. Included in this category may be local political personalities, police chiefs, and heads of significant municipal and national departments or agencies, and tribal or clan leaders.

b. Gray list. The gray list contains the identities and locations of those personalities whose inclinations and attitudes toward the political and military objective to the US are obscure. Regardless of their political inclinations or attitudes, personalities may be listed on gray lists when they are known to possess information or particular skills required by US Forces. These people are the "unknowns." They may be individuals whose political motivations require further exploration before they can be used effectively by US Forces. Examples of individuals who may be included in this category are—

(1) Potential or actual defectors from the hostile cause whose bona fides have not been established.

(2) Individuals who have resisted, or are believed to have resisted, the enemy government and who may be willing to cooperate with US Forces, but whose bona fides have not been established.

(3) Scientists and technicians suspected of having been engaged against their will in enemy research projects of high technology programs.

c. White list. The white list contains the identities and locations of individuals who have been identified as being of intelligence or CI interest and are expected to be able to provide information or assistance in existing or new intelligence Als. They are usually in accordance with, or favorably inclined toward, US policies. Their contributions are based on a voluntary and cooperative attitude. Decisions to place individuals on the white list may be affected by the combat situation, critical need for specialists in scientific fields, and such theater intelligence needs as may be indicated from time to time. Examples of individuals who may be included in this category are—

(1) Former political leaders of a hostile state who were deposed by the hostile political leaders.

(2) Intelligence agents employed by US or allied intelligence agencies.

(3) Key civilians in areas of scientific research, who may include faculty members of universities and staffs of industrial or national research facilities, whose bona fides have been established.

(4) Leaders of religious groups and other humanitarian groups.

(5) Other persons who can materially and significantly aid the political, scientific, and military objectives of the US and whose bona fides have been established.

A-V-3. **Installations.** Installations on the CI targets list are any building, office, or field position that may contain information or material of CI interest or which may pose a threat to the security of the command. Installations of CI interest include—

a. Those that are or were occupied by enemy espionage, sabotage, or subversive agencies or police organizations, including prisons and detention centers.

b. Those occupied by enemy intelligence, CI, security, or paramilitary organizations including operational bases, schools, and training sites.

c. Enemy communication media and signal centers.

d. Nuclear research centers and chemical laboratories.

e. Enemy political administrative HQ.

f. Public utilities and other installations to be taken under early control to prevent sabotage.

g. Production facilities, supply areas, and other installations to be taken under control to prevent support to hostile guerrilla and partisan elements.

h. Embassies and consulates of hostile governments.

A-V-4. **Organizations.** Any group that is a potential threat to the security of the friendly force must be neutralized, rendered ineffective. Groups or organizations which are of concern to CI during tactical operations include—

a. Hostile intelligence, sabotage, subversive, and insurgent organizations.

b. National and local political parties or groups known to have aims, beliefs, or ideologies contrary or in opposition to those of the US.

c. Paramilitary organizations, including students, police, military veterans, and excombatant groups known to be hostile to the US.

d. Hostile sponsored organizations or groups whose objectives are to create dissention and spread unrest among the civilian population in the AO.

A-V-5. **Control Measures.** The CI officer and the G2 need a positive way to keep track of the status of CI targets. Called a target reduction plan, it's a checklist used to ensure targets are seized, exploited, or controlled in a timely manner. The plan is keyed to the scheme of maneuver and lists targets as they are expected to appear. When more targets appear than can be exploited, a priority list is used to denote which target takes priority.

a. Priority one targets represent the greatest threat to the command. They possess the greatest potential source of information or material of intelligence or CI value. Priority one targets must be exploited or neutralized first.

b. Priority two targets are of lesser significance than priority one. They are taken under control after priority one targets have been exploited or neutralized.

c. Priority three targets are of lesser significance than priority one or two. They are to be exploited or neutralized as time and personnel permit.

FIELD MANUAL
NO. 34-80

*FM34-80
HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 15 April 1986

BRIGADE AND BATTALION INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS

Table of Contents

PAGE

PREFACE iii

CHAPTER 1. **The Mission** 1-0

Intelligence 1-0
Electronic Warfare 1-7

2. **Intelligence and Electronic Warfare Resources** 2-0

Battalion IEW Resources 2-0
Brigade IEW Resources 2-15

3. **Command and Control** 3-1

Command and Control Process 3-2
Command and Control Organization and Facilities 3-8
Command, Control, and Communications 3-17

4. **Preparation For Combat** 4-1

Decision-Making Process 4-1
Collection Management 4-4
IEW Tasks 4-9
Reconnaissance and Surveillance 4-41

5. **Combat Operations** 5-0

Prehostility Phase 5-0

*This publication supersedes TC 30-28, 30 June 1977.

COMBAT PHASE

OFFENSIVE OPERATIONS

Brigades conduct offensive operations as part of division and corps offensives, during division and corps defensive operations, as contingency forces, or internally within the context of their own defensive operations. Offensive operations are characterized by aggressive initiative on the part of the subordinate (brigade and battalion) commanders, the ability to make rapid shifts in the main effort to take advantage of opportunities, and momentum to effect deep, rapid destruction of enemy forces. These operations are conducted throughout the brigade and battalion areas of operations and interest.

Brigades and battalions conduct offensive operations to carry the fight to the enemy and to destroy his capability to resist. Depending upon the commander's intent for a particular operation, one or more of the following may be the specified purpose for attacking:

- Destroy an enemy force.
- Secure or seize key terrain.
- Destroy a key element of enemy combat power.
- Fix or contain enemy forces to deprive them of resources or to prevent them from reinforcing elsewhere.
- Deceive the enemy.
- Conduct reconnaissance to gain information about the enemy and terrain.

The destruction of the enemy fighting force and its will to resist is the only way of winning in combat. This purpose is well served by effective and efficient IEW support.

In the offense, certain IEW principles are essential to battlefield success:

- Knowing the battlefield.
- Denying intelligence to the enemy.
- Disrupting and destroying enemy CI and reconnaissance capabilities.
- Maintaining the integrity of IEW operations.

Knowing the battlefield requires detailed intelligence on the enemy, weather, and terrain. Detailed, accurate, and comprehensive IPB begins before initial deployment, is refined during the prehostility phase, and continues, once the battle is joined.

MI battalion assets serve to support economy of force operations by providing early warning and support to deception operations within risk levels acceptable to the commander. MI battalion assets supporting the main attack and economy of force operations must be task-organized according to the tactical situation and METT-T requirements.

Survivability of IEW assets is essential for successful battle outcome. Consistent with security and communications requirements and mission responsiveness, MI battalion assets should disperse to the maximum extent possible. They also apply the full range of OPSEC measures.

C^2 of IEW resources and their effectiveness are directly related. If IEW is to be continuous and responsive, the level, type, and means of C^2 of these assets must be determined early, as defined in Chapter 3.

The primary types of offensive operations include—

- Movement to contact.
- Hasty attack.
- Deliberate attack.
- Exploitation.
- Pursuit.

These operations are described in detail in FM 100-5 and FC 71-100.

Movement to Contact

A movement to contact is conducted to gain or regain contact with the enemy and to develop the situation so that either a hasty or deliberate attack can be made. It is characterized by a lack of information about the enemy; therefore, it is necessary for the brigade or battalion to move using techniques that provide maximum security and afford flexibility. It moves aggressively toward the enemy. Maximum use of intelligence resources is made to find the enemy before the enemy can detect the brigade or

battalion presence. OPSEC measures deny intelligence to the enemy about the friendly forces during movement to contact. When contact is made, combat information and intelligence are used by the commander to determine where to attack, bypass, or defend, and with what force to overcome enemy resistance.

During the movement to contact, IEW resources are employed primarily to provide early detection and location of enemy forces. This effort begins in the planning stage. The BICC, with supporting data from division intelligence sources, expands the division IPB data, relative to the brigade battlefield area, to address the commander's PIR concerning the brigade areas of operations and interest. Through this process, information about the enemy, terrain, and weather are tied together to give the brigade or battalion commander a clear picture of expected battlefield conditions in the areas of interest and operations.

The BICC, with guidance from the S2, defines collection tasks based on the PIR/IR. The BICC prepares mission tasking and transmits it to organic and supporting IEW assets according to C^2 procedures outlined in Chapter 3. Collection missions are also levied through the S3 on combat, combat support, and CSS units within the brigade or battalion. These functions are an inherent part of each operation and are performed prior to, and during, all brigade and battalion operations. IEW resources supporting the movement to contact will normally include interrogators, EW assets, and GSR teams from the surveillance platoon of the MI battalion.

Interrogators move with and support the advance elements. Until contact is made with the enemy and EPW are available, primary sources of information are limited to refugees, line crossers, and other noncombatants. Interrogators determine—

- Locations, size, composition, and direction of movement of enemy forces.
- Enemy unit objectives.
- Location of minefield, obstacles, and antitank weapons.
- Terrain conditions along the route of advance.

EW support to the movement to contact is aggressive, both in planning and execution. Every effort is made to provide continuous coverage of the battlefield. Alternate positions, with LOS along the axis of advance, are selected to enable the EW assets to "leapfrog" forward to support the operation. High terrain to the rear and along the flanks of the maneuver force is identified. Assets requiring long set-up and tear-down times may be best employed in these areas.

EW support is initially provided from positions as close as is tactically possible to the line of departure. As the maneuver elements move forward, their rate of march is computed. This information, along with the estimated set-up, tear-down, and displacement times of supporting EW equipment, allows the ESM and ECM assets to "leapfrog" forward and maintain continuous support for the operations.

ESM collection assets, primarily voice collection teams, intercept and record enemy HF and VHF voice transmissions. Emphasis is placed on detecting forward enemy elements as early as possible. During the movement to contact, intercept priorities include—

- Reconnaissance C^2 nets.
- Tank communications.
- C^2 nets of maneuver units.
- Artillery FS nets.
- Engineer nets.
- REC nets.

HF/VHF and VHF ECM teams deploy and move with the ESM assets during this phase of combat. Although they have no active ECM missions during this time frame, jammers maybe used as passive voice intercept positions to augment existing ESM collection assets.

Surveillance squads and teams move forward with the units to which attached. They support troops or companies or operate with platoons or teams. GSR teams move with the supported unit using "leapfrog" movement, monitoring the terrain

forward and to the flanks of the force to detect enemy activity. They—

- Acquire targets for immediate engagement.
- Provide early warning.
- Search and monitor ambush areas.
- Search areas of conventional fires for signs of enemy activity immediately after firing.
- Cue direct-fire weapon systems.

A type of organization for brigade movement to contact with supporting MI battalion resources deployed is illustrated below.

The movement to contact terminates when enemy resistance requires deployment and a coordinated effort by the main body. All available collection resources are employed to determine the size, capabilities, intentions, and deployment of the enemy force. Tasking of EW assets is redirected to support whatever action the brigade or battalion undertakes.

Hasty Attack

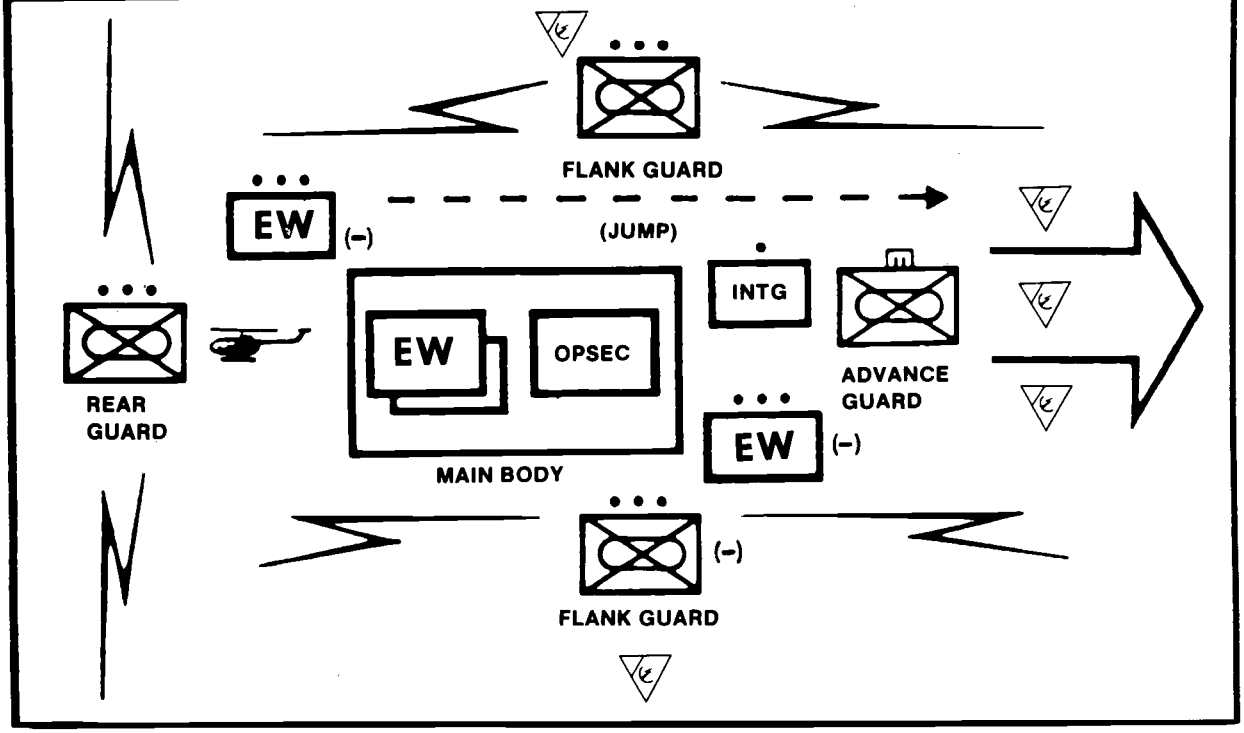
The hasty attack is an offensive operation conducted to defeat the enemy. It also may be conducted to seize key terrain, gain information, or support a deception plan. It is usually conducted following a movement to contact, for which a unit has not made extensive preparations. A hasty attack uses the resources immediately available in order to maintain momentum. From the early moments, every available element of combat and combat support is committed to the attack.

Deliberate Attack

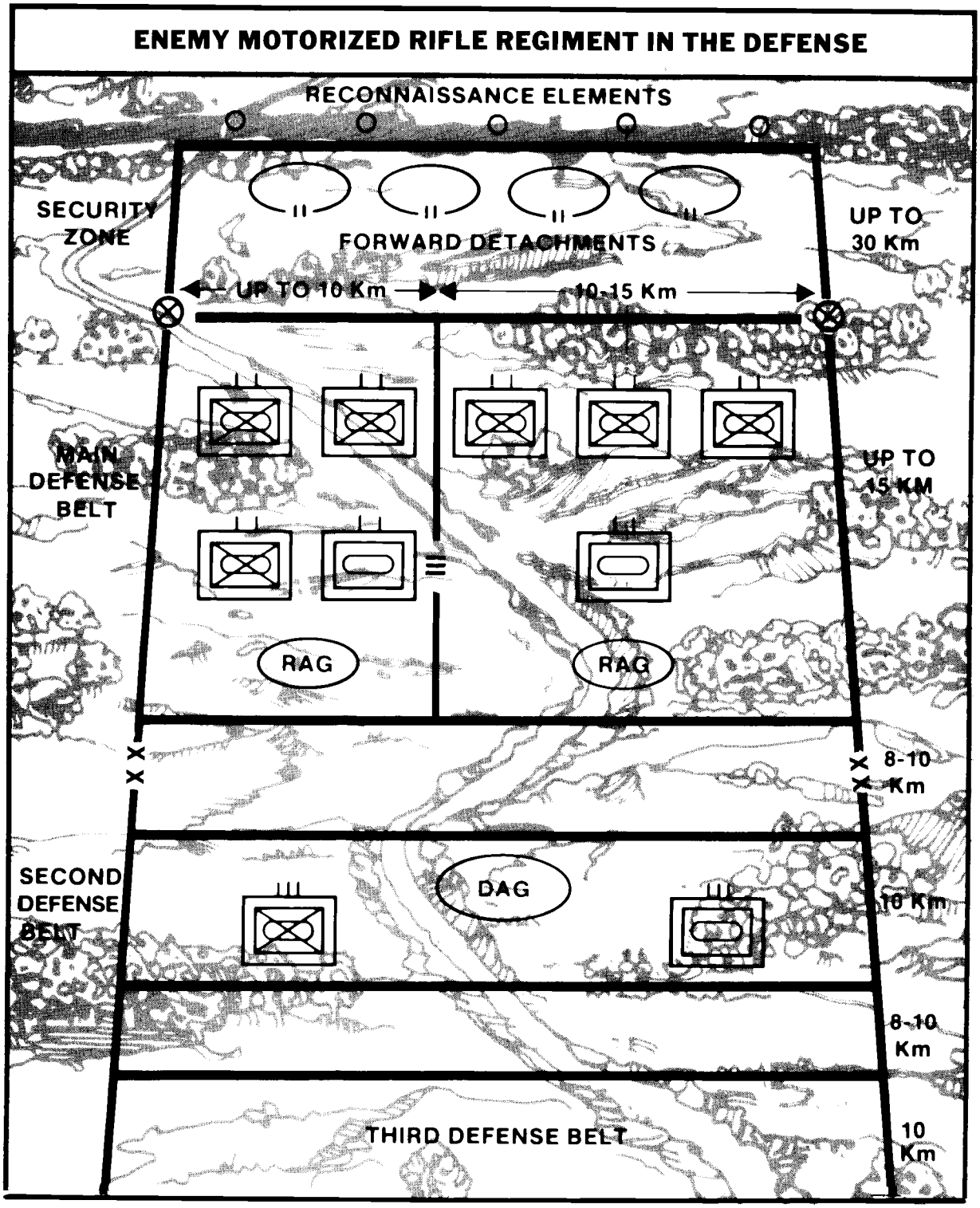
The deliberate attack is also an offensive operation conducted to defeat the enemy. This type of attack, as with the hasty attack, may be used to seize key terrain, gain information, or support a deception plan.

A deliberate attack is planned in detail and is often expensive in terms of manpower, equipment, and supplies. A deliberate attack involves overcoming strong

BRIGADE MOVEMENT TO CONTACT MI RESOURCE DEPLOYMENT DIAGRAM



enemy forces in established positions and is undertaken after thorough reconnaissance, acquisition, and development of targets. It follows an analysis of all other factors affecting the situation. The following illustrates an enemy MRR defense configuration.



It is critical for the S2 to collect detailed combat information and intelligence about the enemy from higher, lower, and adjacent units. Sources of information include patrols, reconnaissance by fire, aerial photography, prisoners, deserters, electronic warfare assets, radar, and remote sensors. Information about terrain can be collected from many of the same resources.

When attacking, the brigade or battalion commander is particularly concerned about the location and commitment of enemy reserves; timing, strength, and location of counterattacks; and time, location, and strength of forces attempting to envelop the attacking forces.

MI resources are initially employed well forward, as far as terrain and the tactical situation permit. As the tempo of the attack increases, certain collection assets become less effective. GSR assets maybe limited to flank screening and rear area security. Ground-based EW assets maybe outrun quickly. When possible, MI commanders "leapfrog" their resources in order to provide continuous coverage. Maximum use of assets must be made to support the attack.

Interrogators locate forward in DS of the BTF. They briefly interrogate EPW, line crossers, and refugees to determine—

- Location and disposition of enemy forces.
- Location of forward line of main defense belt, including location, type, and strength of defensive positions.
- Extent of obstacles and mines.
- Planned operations such as counterattacks, envelopments, and NBC operations.
- Enemy unit objectives.
- Weaknesses in the enemy defense which can be exploited through maneuver, fire, or deception.

OPSEC support teams may support the effort and monitor the posture of the command to detect compromises or conditions that may affect the commander's EEFI. OPSEC is most important before the attack begins. The brigade or battalion must retain the advantage of surprise until it is too late for the enemy to react effectively. Therefore, OPSEC support teams—

- Monitor and observe unit activity to ensure proper employment and coordination of OPSEC and deception plans.
- Monitor deception and countermeasures to detect deficiencies or compromises.
- Perform COMSEC monitoring.

Voice collection teams intercept, record, and provide LOB on enemy voice communications. Combat information is reported immediately for use by FS and ECM elements in accordance with existing SOP. It is also sent via the T&A team to the MI battalion TCAE for processing into intelligence. During the attack phase, high-priority targets include—

- Reconnaissance nets in the security zone.
- C^2 nets between reconnaissance units in the security zone and regiments in the main defensive belt.
- Rocket and artillery FS nets.
- Air defense nets.
- Enemy reserve forces.

Locations of enemy communications emitters in the VHF range are obtained by the TRAILBLAZER DF system. They are then reported immediately to the MI battalion TCAE and the IEWSE of the affected brigade in accordance with procedures outlined in Chapters 2 and 3. TRAILBLAZER is targeted against the same type of targets as the voice collection teams.

Noncommunications collection teams are important to the offense because they detect, identify, and give LOB on enemy radars, noncommunications jammers, and telemetry systems which indicate enemy force disposition and weapon systems to be encountered. Examples of priority noncommunications include—

- Surveillance, countermortar, counterbattery, and air defense radars in the security zone and main defensive belt.
- Nuclear and chemical meteorological radars and telemetry.
- Noncommunications jammers.

ECM teams concentrate their efforts on disrupting or degrading enemy C^2 and FS communications. The teams are tasked to jam—

- C^2 nets linking battalions, regiments, and divisions in the main defensive belt with reconnaissance units in the security zone.
- Critical C^2 links associated with FS and air defense units in the security zone and main defensive belt.
- C^2 nets of reserve forces.

GSRs move with attacking elements, focusing initially on enemy security and forward defenses. They may vector friendly maneuver elements through these gaps. They also monitor the flanks and the gaps between attacking elements.

GSRs support the consolidation of objectives by monitoring possible enemy withdrawals and counterattack routes.

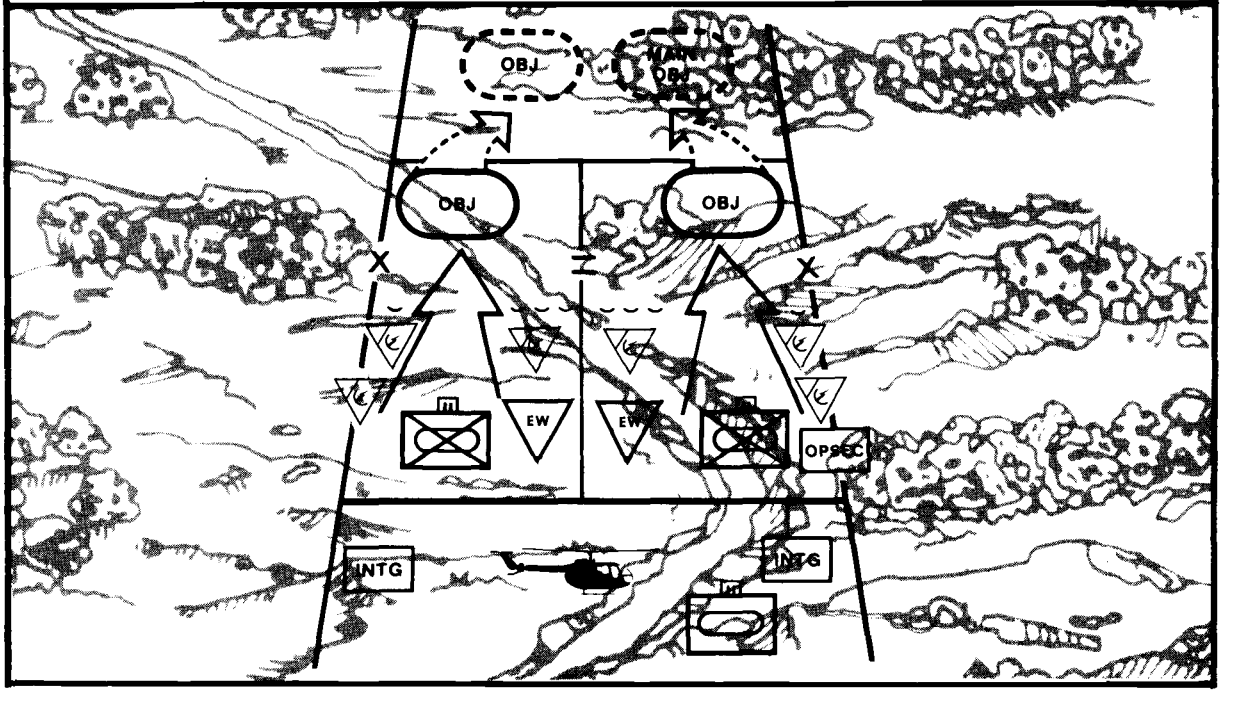
In an envelopment, GSRs detect gaps or exposed flanks in the enemy defenses. A lack of activity is not a sure sign of a gap in the enemy defenses. It is an indicator, however, and can cue other collection systems to locate enemy weak spots. GSRs maybe employed with the enveloping force to provide early warning of enemy activity.

Upon contact with the enemy, GSRs cover areas that the enemy might use for maneuvering forces. They can also vector friendly units that are maneuvering against the enemy. They are especially valuable in providing early warning of enemy maneuver against friendly flanks and attempts at envelopment. They also detect movement of enemy reinforcing or counterattack forces.

By detecting enemy activity, both before and during the attack, GSRs locate targets to determine whether there is any reinforcement, shifting, or withdrawal of enemy units.

MI resources supporting the attack may be deployed as illustrated below.

MI RESOURCE DEPLOYMENT DIAGRAM



Exploitation

Exploitation is the following up of gains to take full advantage of success in battle. It is a phase of the offensive that destroys the enemy's ability to reconstitute an organized defense or to conduct an orderly withdrawal in the face of threatened destruction or capture. It may follow either a hasty or deliberate attack. The brigade can exploit its own success, act as the exploiting force for a higher echelon, or follow and support another exploiting force.

The exploitation is initiated when an enemy force is having recognizable difficulty in maintaining its position. Although local exploitations may appear insignificant, their cumulative effects can be decisive. Exploiting forces can have the mission of securing objectives deep in the enemy rear, cutting lines of communication, surrounding and destroying enemy forces, denying escape routes to an encircled force, and destroying enemy reserves. They require mobility and balanced firepower. Tanks, mechanized infantry, and cavalry, supported by engineers, artillery, and attack helicopters make up the forward elements.

Once the exploitation has begun, it is carried out without interruption to the final objective. The enemy is given no relief from offensive pressure. The exploiting force secures terrain only as necessary to accomplish its mission. Deep attack is used to cut off enemy forces from escape or reinforcement and to inhibit the enemy's reestablishment.

MI resources support exploitation operations by identifying and locating enemy C^2, FS, air defense, and logistical communications and activities. Information gathered from voice collection teams, DF, and EPW interrogators, helps the S2 determine—

- Identification and location of defensive positions.
- Identification and disposition of enemy reserves.
- Enemy unit morale, strength, and logistical status.
- Enemy plans and intentions.

ECM teams are employed to degrade the enemy C^2, and FS communications, adding to the confusion and disorientation caused by the successful attack by friendly fires and maneuver forces. ECM are also employed against the C^2 communication of reserve or reinforcing units to disrupt the enemy reinforcement attempts. This inhibits successful enemy reaction at critical phases during the exploitation.

GSRs continue to support the attack, extending the observation capabilities of forward attacking elements by enabling them to survey distant points or areas of special interest. GSRs also assist the visual observation of attacking units during daylight by making initial detection of partially obscured targets at long ranges.

Pursuit

As enemy forces begin to disintegrate under pressure, exploitation may develop into pursuit. The primary function of pursuit is to complete the destruction of the enemy force which is in the process of disengagement. While a terrain objective may be designated, the enemy force itself is the primary objective.

The brigade conducts local pursuit or is used as the direct pressure or enveloping force of a higher echelon in the pursuit. Exploiting forces must be alert for indications of enemy collapse which enables pursuit. Commanders prepare for pursuit by issuing warning orders, regrouping forces, and providing logistic support. Ground-based IEW elements must be aware of the supported commander's intentions in order to ensure that they are prepared to operate as self-sustaining entities during this period of fast-paced operation.

The speed of advance, the enemy's inability to react effectively, and the dispersion of forces contribute to the security of the pursuing forces. The pursuit is conducted on as broad a front as possible. Forces engaged in direct pressure and eveloping maneuvers are given deep objectives, mission-type orders, and minimum controls. If the attempt to cut the enemy's escape routes fails, a new enveloping force is immediately dispatched. Subordinate and CSS means are decentralized.

The pursuing force employs all available means of ECM to confuse the enemy, to deny him use of his C^2 communications, and to hinder his attempts to consolidate and reorganize.

During the exploitation and pursuit, IEW assets supporting the attacking force continue their missions as originally tasked or as modified by the S2 in accordance with updated PIR/IR to support the commander and the decision-making process. Both operations require that enemy communications, FS, and surveillance systems be located and suppressed or destroyed. This is accomplished with effective coordination and integration of EW and fire and maneuver.

Night and Limited Visibility Combat

All the previously mentioned offensive operations are affected by night and limited visibility operations.

Units attack at night and during periods of limited visibility to continue an attack started in daylight, to achieve surprise and psychological superiority, to gain important terrain for further operations, to use concealment afforded by darkness or limited visibility to avoid heavy losses, or to compensate for friendly air and armor inferiority.

Terrain and weather information must be available to the S2 to aid in planning for night and limited visibility combat. Analysis of the terrain and weather factors affecting trafficability is vitally important to the selection of routes of march for the attack. Terrain features that offer concealment and can be used for heading reference are also important.

IEW collection assets (communications or noncommunications intercept teams, DF, and EPW interrogators) will be tasked to supply information pertaining to enemy defenses such as—

- Location of enemy positions (personnel, weapon systems, routes, and fields of fire).
- Presence and number of searchlights and night vision devices.
- Nature of obstacles, barriers, and bypasses.
- Unoccupied sectors, gaps between sectors, or sectors held by weak forces.
- Overwatch positions for TOWs and tanks.

GSRs maybe oriented along the direction of attack to report and correct deviations for the attacking force. GSRs are more effective when employed with thermal sights to overwatch movement of the attacking forces. The illustration on the following page depicts night attack orientation.

ECM operations employed against C^2 communications of enemy forces in the security zone and the main defense zone are intensified.

ECM, with supporting fires and illumination of the objectives during the critical moment of attack, contribute to enemy confusion and lack of control, and to their eventual defeat.

DEFENSIVE OPERATIONS

The purpose of the defense is to defeat the enemy and regain the initiative. Defense is a temporary measure conducted to identify or create enemy weakness which can be exploited at the earliest opportunity by offensive action. The defender uses fire and maneuver to seek an advantageous position from which to blunt the attack, and concentrates combat power to counterattack. Defending forces are required to hold their positions and terrain and destroy the enemy or cause him to stop or retreat. Defending forces may move to subsequent positions on order or as planned, but their intent—TO DESTROY THE ENEMY AND SEIZE THE INITIATIVE—does not change.

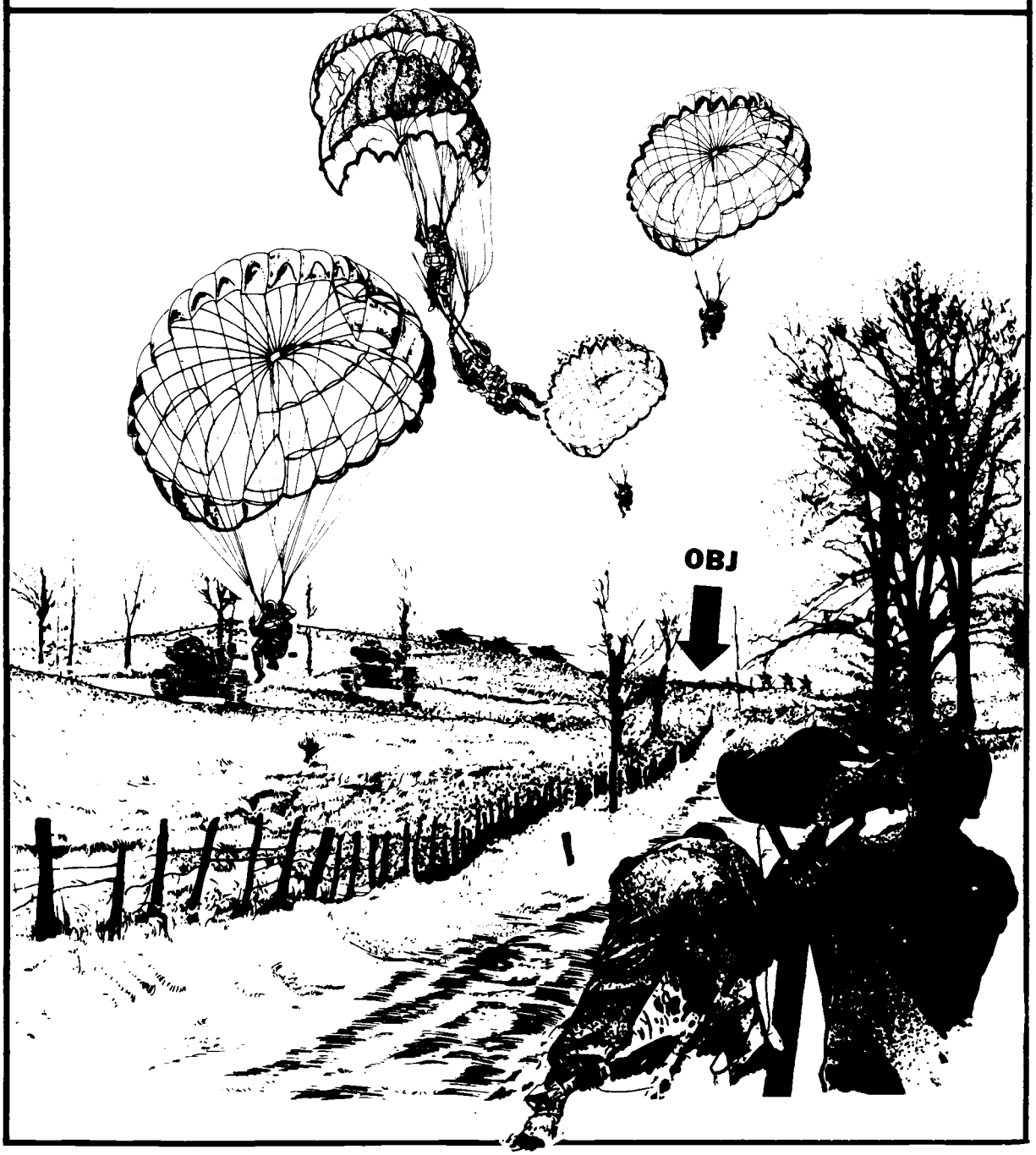
The brigade or battalion will normally defend as part of a larger force. Depending on the commander's intent for a particular operation, one or more of the following may be the specific purpose for defending:

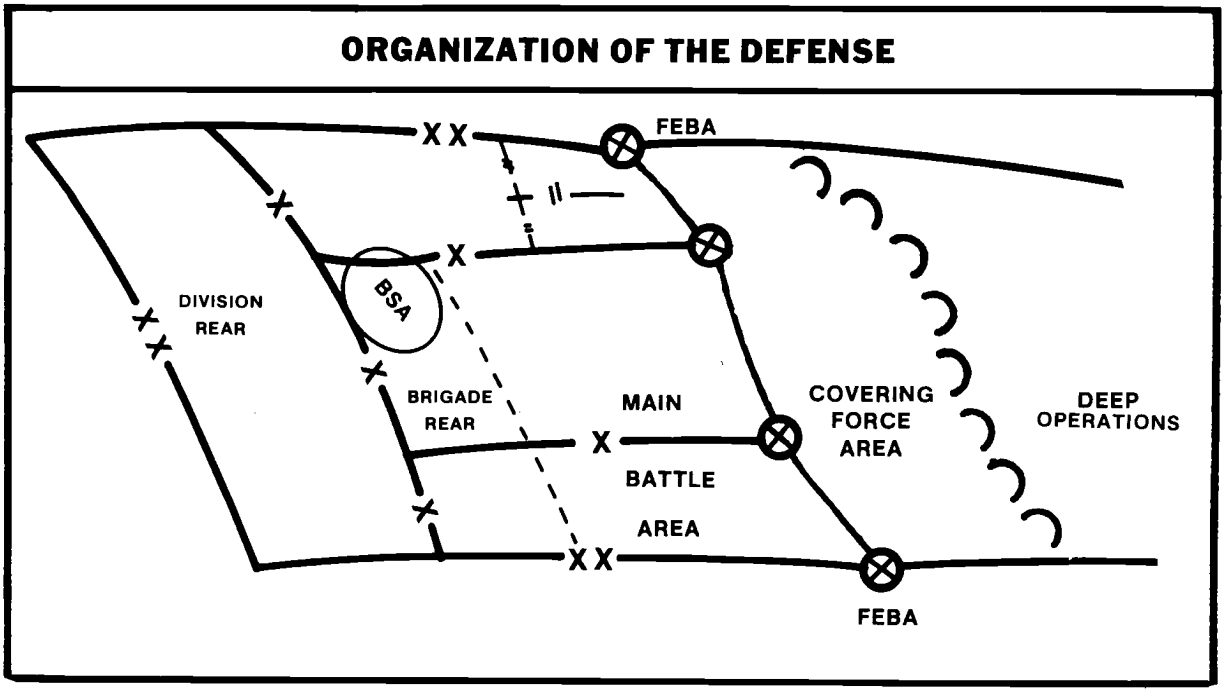
- Concentrate forces elsewhere on the battlefield.
- Gain time without sacrificing the defended area.

- Preserve forces, facilities, or installations.
- Control key terrain.

Brigades conduct close and rear operations. They conduct deep operations-only in terms of participating in the division's deep operational effort. The organization of the defensive battlefield is depicted on the following page.

ORIENTATION IN THE NIGHT ATTACK





The battalion can be employed in each of the operational areas listed below:

- Deep operations.
- Covering force operations.
- Main effort in the MBA.
- Rear area.

The tactical situation and METT-T determine how the commander plans his defensive efforts. The MI resources to support the overall operation are task organized and allocated based on the need. These resources may either be GS to the division or DS to the brigade in whose area they are operating.

The IEW principles discussed in offensive operations apply to the defense as well.

- Knowing the battlefield.
- Denying intelligence to the enemy.
- Destroying and disrupting enemy C^3I.
- Maintaining integrity of operations.

IEW support enables the commander to see the battlefield clearly. Collected information from IEW assets is analyzed at the BICC to provide the commander with early warning of enemy intentions and targets for fire and maneuver forces. IEW assets must also be alert to enemy deception attempts and report them in sufficient time for the commander to act effectively. It is essential, therefore, that the IEW assets be task organized and deployed early to provide intelligence, combat information, and targeting data to support the division's deep operation, the covering force, the MBA, and the rear area.

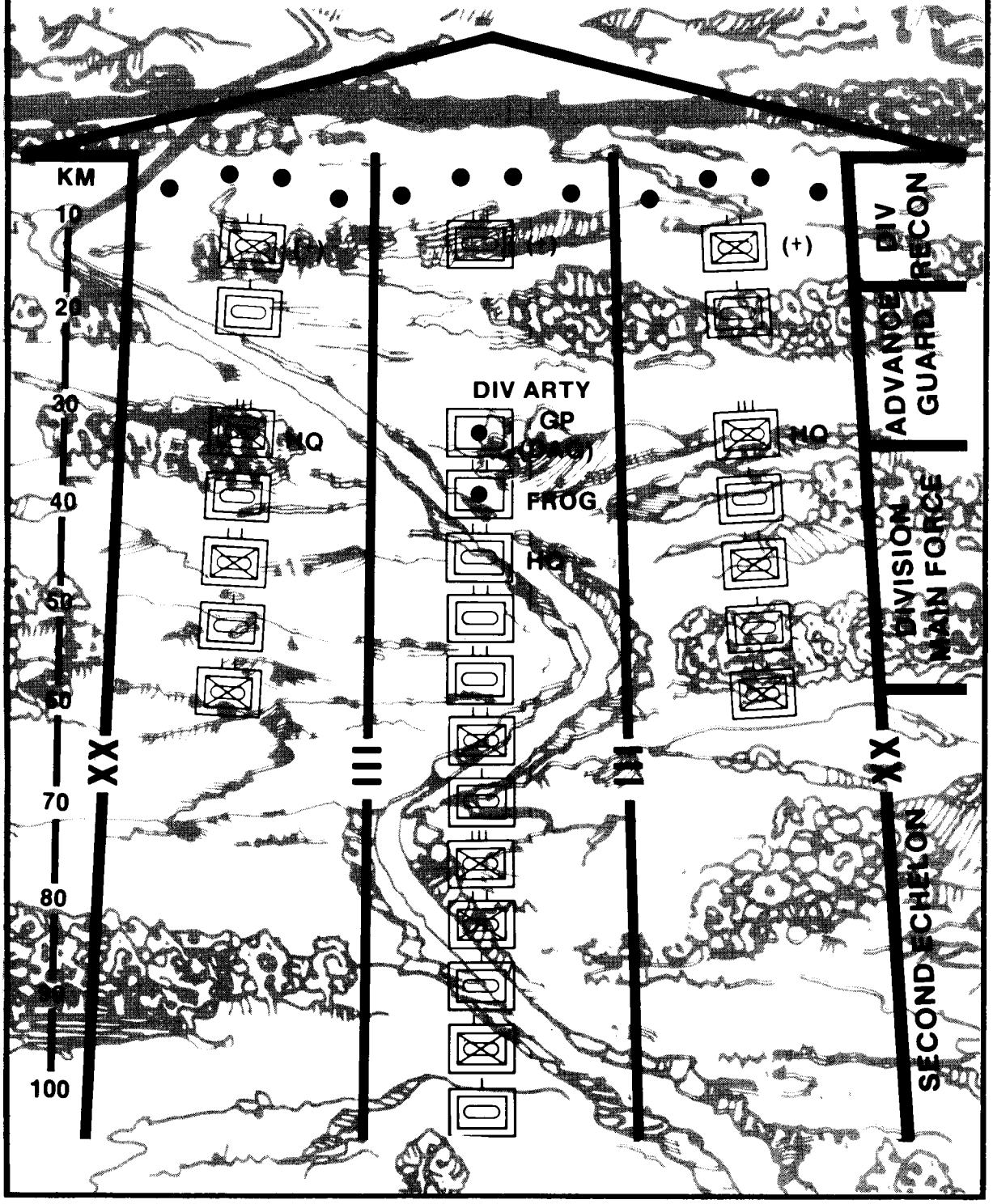
The first task, once the battle begins, is for IEW assets to identify and collect against the enemy's main effort as early as possible. Enemy methods of movement and attack must be understood. to identify the enemy's main effort.

The following figure depicts a motorized rifle division (MRD) in its movement to contact. The tank division (TD) is similar.

Once contact is made, the enemy commander will deploy his maneuver elements for a deliberate attack.

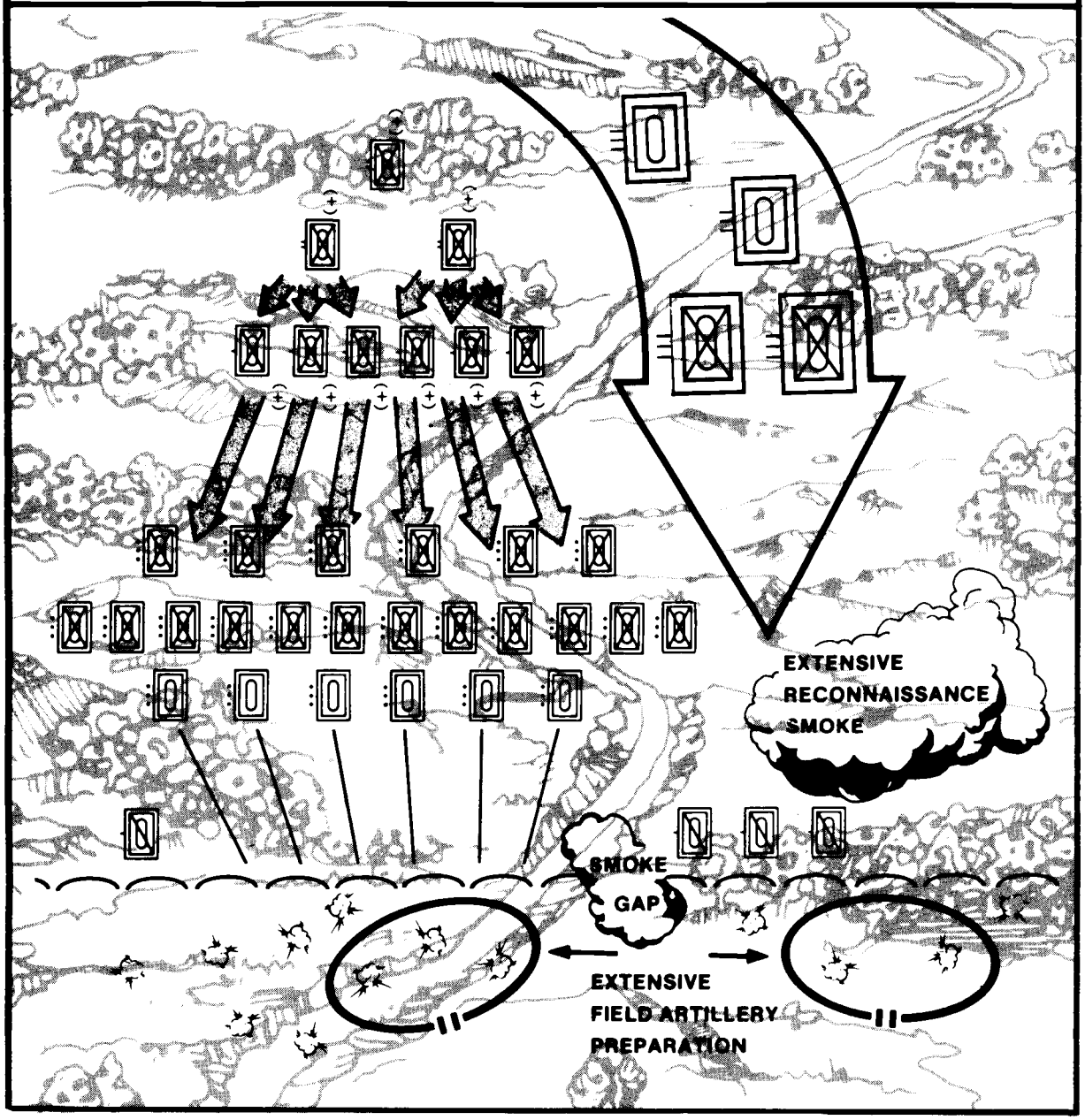
In the offense, enemy forces concentrate numerically superior forces for a combination of frontal attacks, envelopments, holding attacks, and deep thrusts. Normally, a

TACTICAL MARCH OF AN ENEMY MOTORIZED RIFLE DIVISION



division will select one main and one secondary axis of attack. The entire division may move along a single axis if that is necessary to achieve force superiority. Rather than attempting to seize key terrain, it concentrates on breaking through weakly defended or unoccupied areas to carry the battle to the rear. Momentum of the attack is sustained through echelonment of forces and extensive artillery fires. The following figure depicts an enemy's configuration for deliberate attack.

ENEMY DIVISION DELIBERATE ATTACK



Deep Operations

The deep operation is used by the division and higher echelons to affect the closure times of follow-on elements and create windows of opportunity for decisive action against leading enemy echelons. Brigades and battalions participate in deep operations as part of the overall division force. Areas of interest and operations extend forward of the FLOT far enough to give the commander time to identify approaching enemy forces, assess his options, and execute operations accordingly. The deep component of the operation begins before the enemy closes with the close-in maneuver forces, goes on throughout the covering force and MBA battles, and usually continues after direct contact between forces has ended.

In conducting the deep operation, the commander's intelligence collection effort is focused by making specific demands on the intelligence system. As enemy formations approach the FLOT, the commander monitors their movement, seeks high-value targets, disrupts and delays them, and modifies his defensive plan as necessary.

The means available for deep attack may be limited in number and effect. Special care is taken to use deep fires and maneuver efficiently to obtain effects which contribute directly to the success of the overall defense. Air-delivered weapons, tactical nuclear weapons, air maneuver units, and special operation warfare forces are the chief weapons of the deep operation, though other maneuver forces may be used. Generally, more sensors and weapons become available as the enemy nears the FLOT.

Effective employment of these means depends on careful planning and IPB at the division level before the operations begin and on a responsive surveillance operation once operations are under way.

The brigade S2 receives intelligence products from higher, adjacent, and supporting IEW resources to satisfy the brigade commander's deep operation information requirements.

IPB in the brigade's area of interest for the deep operation was initiated prior to deployment. This process continued during the prehostility phase with the majority of the situation and target development data being produced by division, corps, and EAC assets. Aerial COMINT and ELINT systems collect information on, and locate, enemy C^2 communications and noncommunications systems. Long-range patrols, when available, provide detailed HUMINT on activities and locations deemed critical to the deep operation. This data is passed through corps and division intelligence channels to the brigade S2 as needed.

During the defense, the brigade is concerned with the approaching enemy force composition, disposition, strength, rate of movement, and intentions in its area of interest. As enemy formations approach the brigade's AO, the commander monitors their movement through collection, analysis, and reporting from division; seeks HPT; and initiates deep attack options against follow-on battalions and first-echelon sustainers. EW and REMS resources provide the S2 with data on approaching forces which, when coordinated with the FSO and S3 and integrated into the fire and maneuver plans of the brigade, allows for destruction, disruption or delay of these forces.

ESM resources support the deep operation by–

- Locating and monitoring C^2 nets between first- and second-echelon battalions, regiments, and divisions.
- Locating and monitoring C^2 nets associated with artillery and rocket units, especially those with NBC capability.
- Locating and monitoring enemy air defense nets.
- Jamming C^2 communications of reserves of second-echelon battalions and regiments.
- Jamming communications nets used to coordinate passage of lines, maneuver, and traffic control.

Noncommunications collection teams detect, identify, and give LOB for enemy noncommunications emitters in the deep operations area. This emitter information assists in the situation and target development process within the BICC. Priorities include:

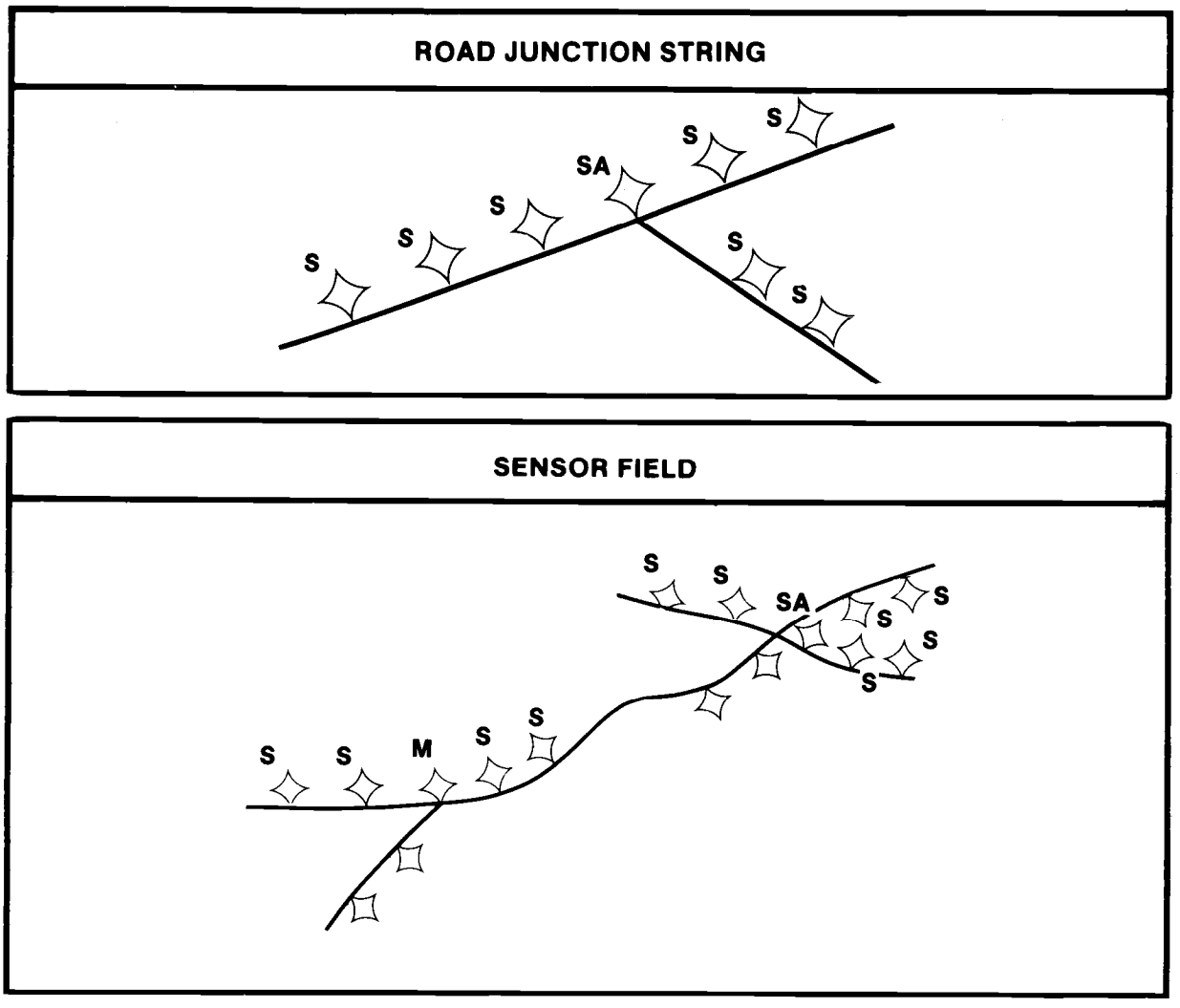
- Surveillance radars of second-echelon battalions.

- Air defense radars of second-echelon units.
- Meteorological radars in the deep operations area.
- Counterbattery radars.

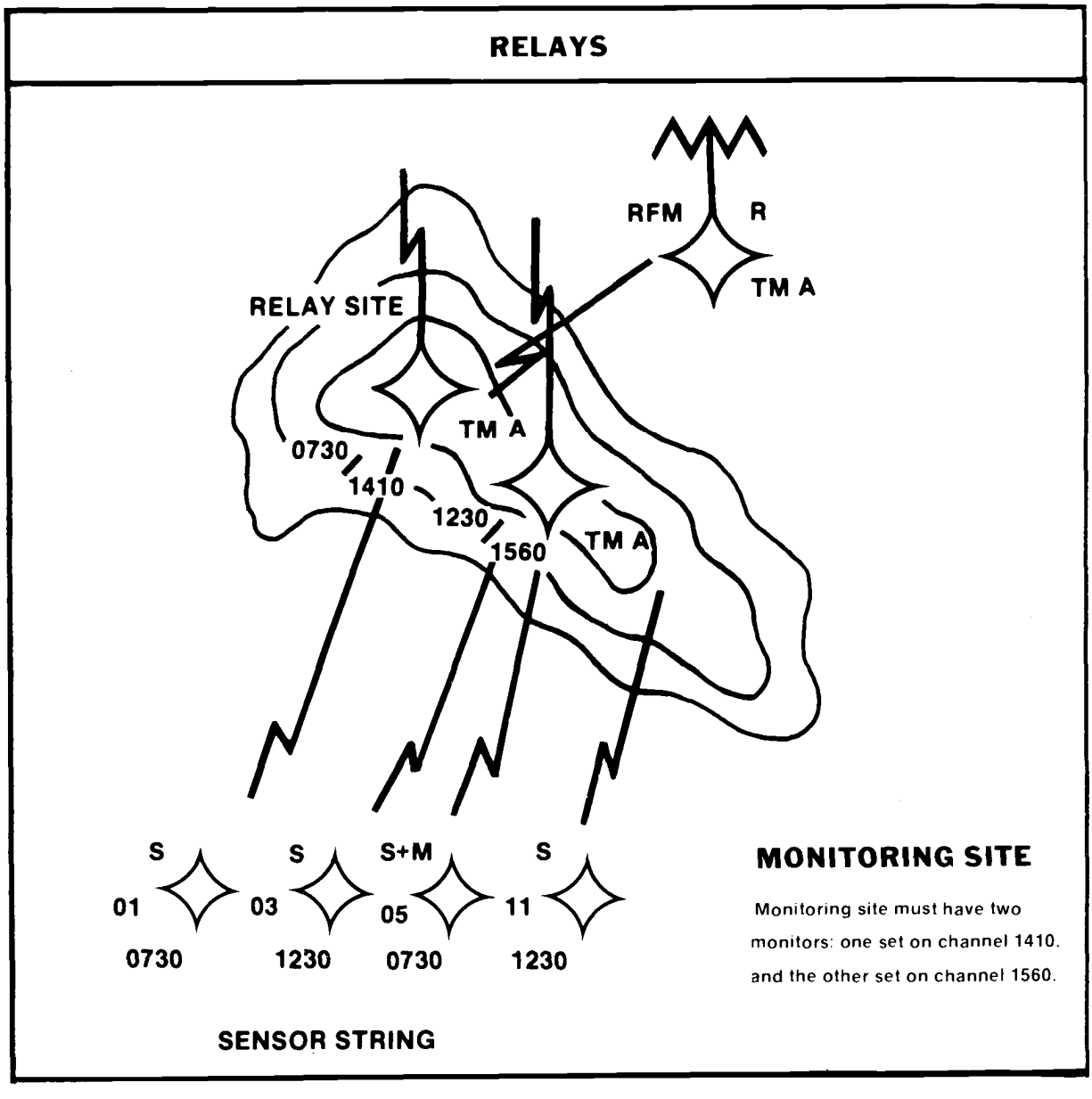
REMS provide an additional source of information for the ground commander that can be used for the production of intelligence and timely, accurate target acquisition data. To support the deep operation, REMS maybe emplanted deep in the enemy's rear area to provide indications of reinforcement. Sensors may be hand-emplaced by maneuver-unit patrols, long-range reconnaissance patrols (LRRPs), long-range surveillance operations, or by sensor teams. For monitoring movement in the enemy's rear area, especially at specific NAIs, the REMS can be employed at specific road junctions or as sensor fields over a wider area.

The road or trail junction string includes two seismic sensors placed at each end of the three approaches of a Y-type road or trail junction. A rule of thumb is to place two seismic sensors on every approach and confirming sensors at all road junctions or intersections. This is illustrated by the following.

A sensor field is two or more sensor strings employed to monitor two or more specific locations within an area of interest, as shown here.



There are two situations in which sensor relays must be employed. The first is when the sensor implant location is not within radio LOS of the monitoring site. The second is when the distance between the sensor implant location and the monitoring site is greater than 50 miles or 80 kilometers. The current relay, used with remote sensors, is the expendable relay AN/GRQ-21. It will receive digital sensor signals on one channel and retransmit this signal to the monitor site on a different channel. The relay receiver channel must be the same as the sensor's transmit channel. Because the relay transmits the sensor signal on a different channel, the RF monitor at the monitor site must be set on the same channel as the relay's transmit channel. Because the relays can only receive and retransmit one channel, each sensor string will require two relays to retransmit all sensor information. In most situations, each sensor string is employed with a two-channel mix which will require two relays, as down by the example below.

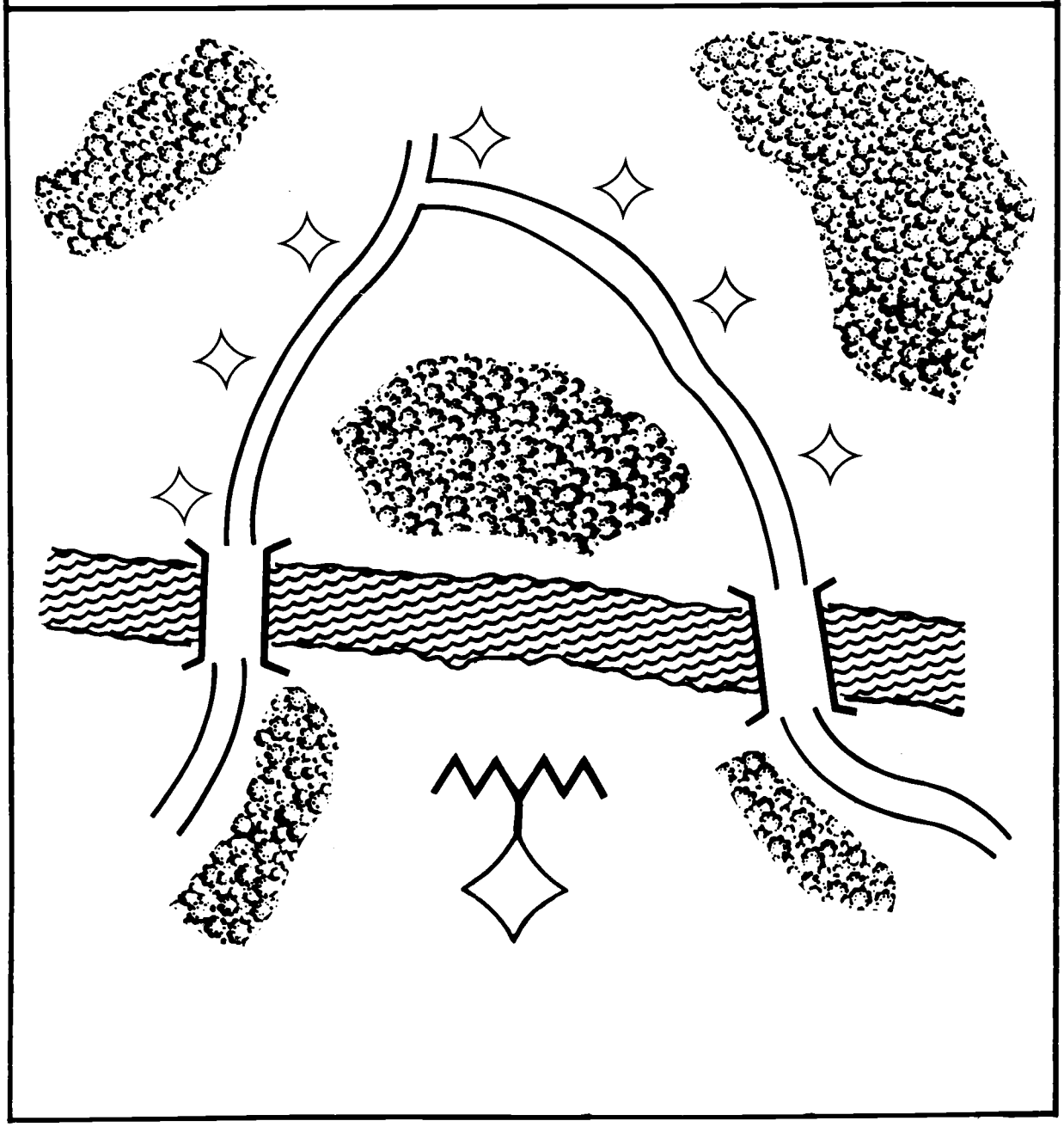


The timeliness and accuracy of sensor-derived data make REMS an excellent target acquisition resource. The REMS team emplaces sensors near predesignated target areas and reports activations to the FIST. Properly employed, REMS can indicate the type, size, number, direction of movement, and speed of the target.

A typical target acquisition sensor employment is shown below.

It is the fusion of all the IEW collected data and its integrated use in target and situation development that allows the commander to see deeply and conduct the deep operation.

TARGET ACQUISTION



Covering Force Operations

The covering force is formed by the forward security echelons. It defends or delays and withdraws in a "staggered" sequence, when appropriate.

The fundamental purpose of the covering force in defense is to serve as the forward security echelon. It occupies a sector far enough forward of the FEBA to protect MBA units from surprise, to allow MBA forces to move to meet the enemy attack, to prevent the delivery of enemy medium-range artillery fire against MBA units, and to deceive the enemy on the location of the main defensive positions. The mission of the covering force is to gain and maintain contact with attacking enemy forces and to develop the situation.

In many instances, corps and division commanders establish a strong covering force to form the first echelon of a defense in depth. The covering force conducts a major operation to destroy leading enemy formations, causes the commitment of follow-on battalions or regiments, causes repositioning of enemy artillery and air defenses, and thus forces the enemy to disclose his main effort. While the covering forces are fighting the enemy's leading echelons, the next higher level of command conducts the deep operation against enemy follow-on forces and prepares for the main operation based on covering force and deep operation developments.

The size and composition of the covering force area depends on the mission, enemy, terrain, and available forces. These factors take on added significance and complexity, depending on the attack mode chosen by the enemy, the depth and width of the area available for covering force operations, and the time required for MBA defenders to get set for action. The covering force is normally tank-heavy. A defensive covering force operating in front of a division could well consist of four or five tank-heavy battalion task forces, attack helicopters, field artillery, air defense, and engineer units.

IEW resources that are used to identify the enemy's main effort will be deployed in the covering force area as dictated by their capabilities and limitations outlined in Chapter 2, and by task organization.

Target confirmation, validation, and development is conducted in accordance with the division and brigade collection plan. The EW resources will respond to the brigade's collection plan through the IEWSE and EW platoon headquarters, rather than directly from the S2 as GSR, REMS, CI, and interrogation assets would.

The covering force area, where IEW resources will be initially deployed, begins at the FLOT and extends rearward to the FEBA, This is where the covering force performs its four basic tasks of—

- Deceiving the enemy as to situation.
- Forcing the enemy to deploy from his march formation.
- Stripping away enemy air defenses.
- Delaying the enemy.

MI resources in the defense will be based on the MI battalion in support of the heavy division, because of the preponderance of this type of unit in the US Army. Light divisions, air assault and airborne divisional MI assets, although different in numbers, will be employed similarly to the heavy division in defensive operations. Differences will be discussed later in this chapter.

In the defense, most combat and intelligence elements are relatively static until contact is actually made with the enemy. GSR and EW elements, on the other hand, because of their unique electronic signatures, must continuously reposition themselves to avoid enemy REC activities and subsequent destructive fires.

MI assets are deployed to support the covering force operations. RSTA assets extend the capabilities of the covering force in the collection of vital combat information and intelligence, based on the commander's PIR and IR.

Covering force area operations are enhanced when the two types of GSR teams are deployed together tactically. The AN/PPS-5 teams can be positioned to exploit their long-range capabilities, while the mobility and quickness of the AN-PPS-15 can cover areas immediately beyond the

FLOT. Both types of GSR teams are used for—

- Search missions. Search for enemy activity on likely avenues of approach or withdrawal, attack positions, and assembly areas.
- Point surveillance. Monitor point targets such as bridges, defiles, or road junctions to detect movement in and around the point. Similarly, this type of surveillance can be conducted to cover gaps between friendly units and key terrain where observation posts might be established.
- Route surveillance. Scan roadways or portions thereof to detect and obtain information on traffic density, rate, direction, and type of movement.
- Control and coordination. Assist in the control of units, especially during the night operations, by monitoring and vectoring the movement of friendly RSTA and warning them of enemy and other friendly activities along their routes.
- Fire control support. Acquire targets for fire missions and track the advancing or retreating enemy to permit the timely shifting of fire. When coordinated with final protective fires and illumination plans, GSR teams are used to locate the enemy and alert the supported unit so that fires, illuminations, and pre-positioned munitions can be employed at the appropriate time and survey target areas immediately following the lifting of fires to detect any remaining activity.
- Observation. Vector friendly maneuver while concurrently searching for enemy activity during periods when visibility is limited or obscured.
- Riverine defense. Detect and monitor the movement of both friendly and enemy watercraft.
- Perimeter security. Enhance security and provide early warning of intrusions, movements in likely routes of approach toward the perimeter, and unusual or suspicious activities near long stretches of pipeline or LOCs. The AN/PPS-15 team is equipped ideally to accompany motorized security patrols and provide early warning of suspicious activities along the patrol's intended route of march.

GSRs with EW assets often can help locate the enemy's main effort by comparing activities noted in other parts of the CFA. They can be used to anticipate enemy maneuvers, establish the depth of the enemy offensive, or uncover an enemy feint or demonstration. They cover gaps between friendly units and monitor exposed flanks and other critical areas, such as the rear.

During the covering force operation, REMS can be used with GSRs to provide flank security. When employed on lightly defended flanks of maneuver elements, sensors provide early warning of enemy attempts to conduct envelopments. When employed in this manner, REMS will permit economy of force by reducing the number of troops needed to protect a unit's flank in the CFA.

EW support to the CFA is task organized to accomplish four primary tasks:

- Provide early warning.
- Assist in targeting.
- Augment combat power with ECM.
- Support the commander's deception plan (when such plans exist).

EW provides early warning and targeting assistance through ESM. ESM consists of communications and noncommunications intercept and direction finding and is described along with ESM systems in Chapter 2. Early warning may also be provided the brigade and battalion by corps and EAC aerial ESM assets.

These assets can provide early warning of enemy troop disposition, movements, and intentions at a much greater range than those ground assets organic to the division. Requests for tasking of these elements originate at the division G2 or G3. Brigades and battalions receive intelligence from these missions through normal intelligence channels.

As enemy units close on the CFA, the brigade and battalion resources assume the

task of early warning, identification of the enemy's main attack, and target development.

Voice collection teams are deployed 2 to 5 kilometers behind the FLOT, coordinating with maneuver elements for deployment sites. The voice collection teams require radio LOS along probable enemy avenues of approach for best utilization.

DF elements of TRAILBLAZER require the same considerations in siting as the voice collection assets. The voice collection elements are found solely in the brigade area and are tasked to support only avenues of approach within that brigade. TRAILBLAZER, on the other hand, will be located not only in a brigade area but also straddling brigade lines.

By its nature, TRAILBLAZER requires a large area for deployment and, because of its unique electronic signature, must continuously redeploy throughout the MBA to avoid enemy REC and subsequent fires. To retain continuity of intercept and direction finding, TRAILBLAZER must use the "leapfrog" method for redeployment. To accomplish this, for example, one MCS and one RSS will deploy to new positions while the remaining MCS and two RSS hold their positions and continue with tasking. The SPP headquarters element will deploy with the same MCS throughout deployment to maintain continuity. When the redeploying elements are in position and in communications on line with TCAE and SPP HQ element, the remaining MCS and RSS will redeploy. The SPP headquarters element will at that time pass control of the mission to the MCS that has communications with the TCAE. When the SPP headquarters element is in its new location, it will reassume control of the mission. This leapfrog concept is shown on the following page.

Priority of effort for the SPP is to the interdiction battle in the CFA. As the covering force operation is handed off, priority of support shifts to forces in the MBA. During operation in the MBA, targets include—

- NBC delivery systems.
- HVT and HPT as directed by the commander.
- Enemy jamming operations.
- CPs.
- Fire support C^2 elements.
- REC systems.

The voice collection elements determine branch, echelon, location (LOB), direction of movement, and capabilities of enemy combat, and combat support, targets.

At the direction of the TCAE, voice collection elements in GS to division can be used to augment the SPP by acting as additional RSS with separate intercept capabilities. This increases the DF baseline and offers more LOB data for a more accurate emitter location. Drawbacks to this augmentation are a conflict of tasking to the voice collection site, and communications equipment incompatibility. The voice collection team must use FM VHF transceivers and cannot talk directly to the MCS computer. LOB data must be manually collated at the SPP or TCAE to be incorporated with the TRAILBLAZER product.

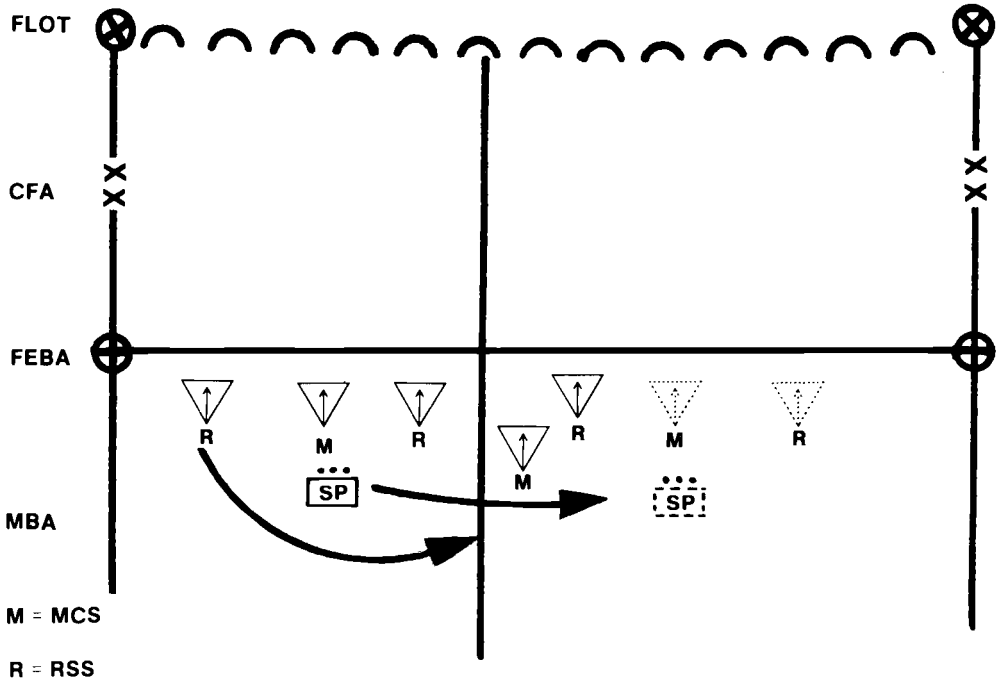
This product, target emitter locations, is used by the S2 with target information from other sources; GSRs, imagery interpretation, voice intercept and noncommunications intercept, to provide a target list to the brigade and battalion FSEs for fire missions.

The light, air assault, and airborne divisions will not have an SPP and will rely on the voice collection team equipment for the DF missions.

Noncommunications intercept elements require the same siting considerations as the voice collection and SPP elements. The LOB, cut, and fix data produced by TEAMPACK are correlated with GSR, countermortar/counterbattery radar, communications intercept, and DF, compared to the brigade and battalion target list, and fed to the FSE and TACP for suppression, fire, and air strike.

The ECM elements in the CFA and MBA will be deployed in the battalion area and must coordinate closely with the battalion for sites. The C^3 facilities supporting enemy RSTA, REC, and both division and regimental artillery groups are HPT for all ECM resources as enemy forces enter and

TRAILBLAZER DEPLOYMENT: LEAPFROG



advance through the CFA. COMJAM operators selectively jam critical communications links. They use both conventional and special operating techniques and procedures which are specifically designed to delay and confuse enemy commanders and fire control operators. Enemy maneuver C^3 facilities are also attacked on a selective jamming basis. Frequently, two or more jammers alternately engage the same target. This not only increases the effectiveness of the ECM attack but decreases the danger from enemy REC and subsequent fire. Frequent redeployment is also required to reduce the danger of enemy fire.

During the defense, the ECM assets are most effective because of the enemy's heavy reliance on C^3 for control of the attacking forces.

ECM has many methods at its disposal for the disruption and denial of enemy communications. The ECM equipment available to the friendly commander can, after detection and identification of enemy HPT, block transmission at regiment to battalion levels. Nuisance intrusion by ECM operators may be conducted to confuse the enemy and disrupt his advance, provide false data to be acted upon by enemy ADA and FSE, and require the enemy to waste valuable time confirming radio communications.

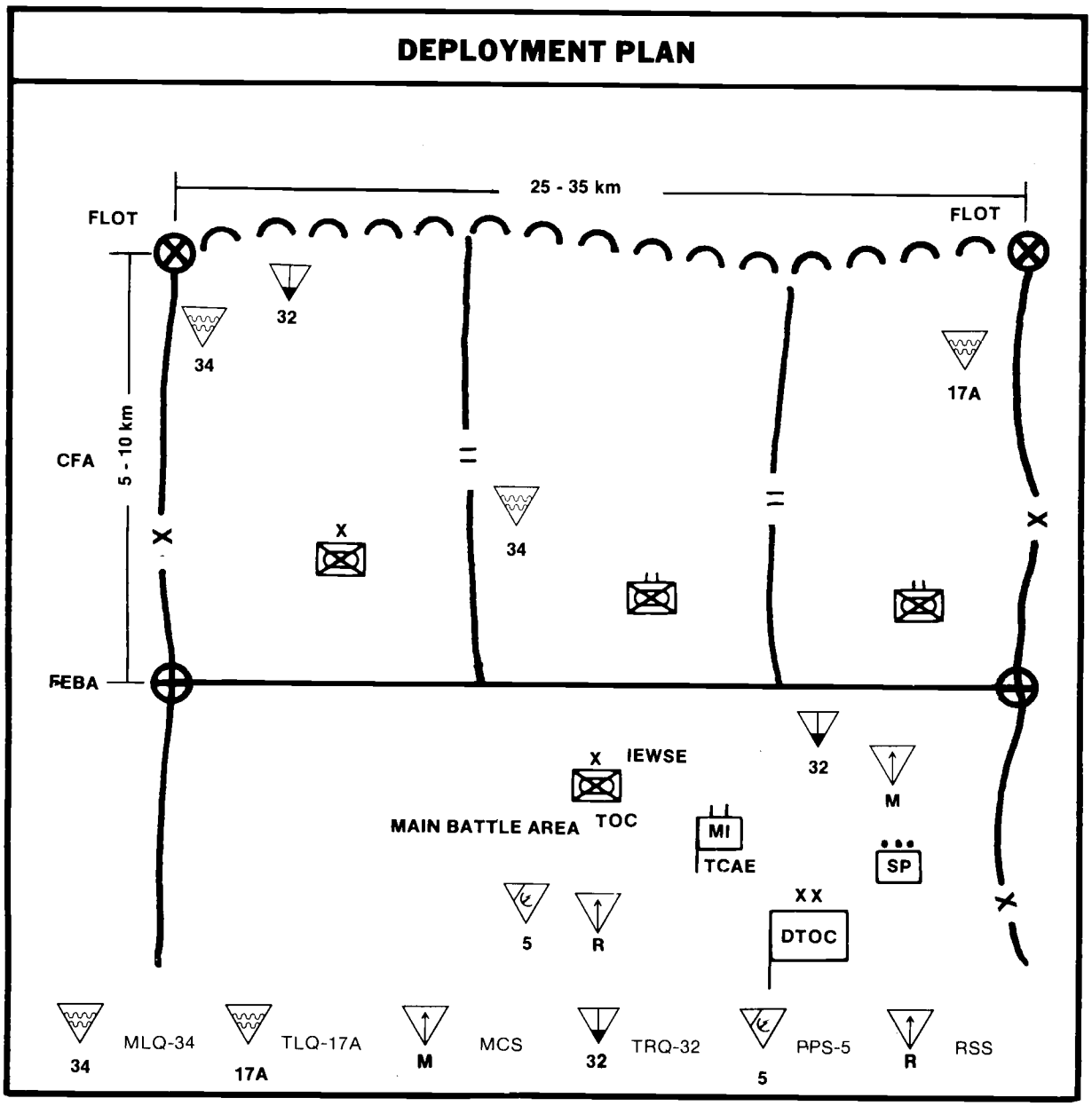
Enemy barrage jamming of friendly communications will be present and heavy during their offense. ECM assets can and should be used to provide high-power "burn-through" VHF communications for the brigade and battalion upon tasking from the TCAE and the brigade and battalion commanders.

Deployment of ECM assets is designed to provide not only ECM capability but ESM augmentation.

The high-powered and more mobile TACJAM resources may be developed forward in the CFA to attack close-in and distant

HPT in the enemy's force and to augment the division's or brigades' overall collection effort. The lower-powered and less mobile TRAFFIC JAM resources may be deployed near the FEBA and will be used for close-in jamming missions. Also, because of its frequency spectrum scanning capability, TRAFFIC JAM is used to assist voice collection tasking efforts.

A typical deployment plan in a brigade area of the CFA is shown below.



The light, airborne, and air assault divisions will not see the concentration of equipment seen by the heavy division, and may not be able to saturate their AO. The types and numbers of equipment will be used in the same way and will provide the same intelligence and information as the heavy division's assets.

When dictated by the tactical situation, the voice collection, ECM, and noncommunications intercept teams will deploy to the MBA and take up sites along the FEBA to provide the same EW support as is done in the CFA.

ECM, voice collection, DF, and noncommunications coverage of the battlefield must remain constant. To remain constant, the leapfrog method of redeployment used by TRAILBLAZER will be used by the other elements to reach the MBA.

To preclude being left behind during withdrawals, the EW platoon leaders ensure that coordination is maintained with the maneuver element in whose area the EW assets are deployed.

The decentralized, fluid nature of the covering force operation requires interrogation support at the lowest echelons, often at troop and company level. This requires DS interrogation teams from supporting MI companies, battalions, and the corps MI brigade. Questioning of civilians and EPW is brief and conducted to gain information of immediate tactical value. Interrogators gather information about the identification, composition, location, direction of movement, strength, and capabilities of enemy forces involved in the immediate covering force operation.

Close Operations

In his close operations, the brigade commander concentrates on the interrelationships of the terrain, the estimated enemy, the capability of the battalion's direct fire weapons, and supporting fires. The brigade commander's organization for combat considers the capabilities of his unit and their employment to stop, delay, or attack the enemy.

The analysis of the terrain influences the concept of the brigade commander's plan for battle. From the defensive perspective, the terrain offers open maneuver spaces and chokepoints or restrictive maneuver areas. The S2, assisted by the BICC, continually updates the SITMAP. Using weather and terrain data and the IPB process, BICC personnel analyze the battlefield to estimate the course of action the enemy force will take during the attack in the MBA. This analysis is aided by IEW input from MI battalion resources deployed in the brigade AO.

Generally, MI support to the brigade battle requires a high degree of centralized control and decentralized execution. Use of the IEW company team concept is especially appropriate in the close operation since it maximizes both control and execution of IEW support. Corps assets may augment the assets in the company team:

Interrogation teams are deployed at the brigade collection point. When necessary, they may be deployed at battalion level. Screening operations and interrogations are conducted at the brigade collection point to gain information of immediate tactical value about—

- Locations, types, and disposition of enemy forces, including reserves.
- Enemy unit objectives.
- Location of the enemy's main attack.
- Enemy weaknesses.
- Enemy tactics and intentions, to include use of NBC weapons.

When requirements exceed the capabilities of organic interrogator assets, augmenting interrogation teams may be provided by the MI brigade (corps).

OPSEC in the close operation is essential to maximize the natural advantages of the defense. OPSEC support teams may operate throughout the brigade or battalion area. When so deployed they advise and assist the brigade S3 on matters concerning OPSEC and deception. OPSEC teams—

- Monitor the execution of OPSEC and deception measures approved by the commander or S3.
- Recommend countermeasures to reduce the potential of compromise of EEFI.

- Perform COMSEC monitoring.
- Recommend and assist in planning deception operations.

GSRs continue to be used as they had been during covering force operations. Targeting enemy assault forces, overcoming obscurations caused by weather or battlefield smoke, and covering gaps and exposed flanks are a few of the tasks performed by GSR teams. When deployed in gaps or on flanks, the GSR teams increase the combat power of the defending elements by providing early warning of enemy activity and by targeting the enemy force at maximum range. GSRs can often help locate the enemy's main attack by comparing activities in various parts of the sector. They can anticipate enemy maneuvers, establish the depth of an enemy offensive, or uncover an enemy feint or demonstration.

REMS maybe effectively used in defensive operations as an early warning system to provide indications of enemy movement and location. The amount of activity detected by the sensors may provide indications of main or supporting attacks, feints, or diversions. Since activity will be at its peak on the battlefield, sensors may be saturated with activation and may not be able to provide anything other than warnings of imminent attack. Other than this disadvantage, defensive uses may include any or all of the following:

- Targeting.
- Detection of enemy patrol activity.
- Detection of enemy infiltration.

Communications and noncommunications intercept collection, and direction finding resources concentrate their efforts against enemy first-echelon forces and the potential introduction of the second-echelon ESM resources (both communications and noncommunications), target manuever, FS, air defense, and other critical elements of the enemy force. Intercept and DF resources in the conduct of close operations concentrate on—

- Enemy maneuver nets.
- Enemy REC elements, especially communications jammers.
- Regimental and division FS systems.
- Surveillance radars with first-echelon battalions.
- Air defense radars with first-echelon regiments.
- Countermortar and counterbattery radars.
- Meteorological radars.

Rear Operations

A major tenet of Soviet military doctrine is to disrupt an adversary's rear area through the use of agents, saboteurs, terrorists, special action, and diversionary forces; attacks by maneuver units; and aerial and artillery fires. Soviet heliborne or air assault operations are the primary means of attacking or infiltrating the rear area. Enemy doctrine stresses the use of battalion-size units conducting heliborne operations to depths of 50 kilometers. Airborne assault operations, up to division size, may be introduced up to depths of 300 kilometers in support of strategic objectives. Attacks against rear area targets are carefully coordinated as an extension of combat in either the CFA or MBA. The goal of heliborne operations in the brigade area is to degrade friendly support and sustainment of CFA and MBA battle and to divert forces from these areas. These attacks also contribute to the demoralization of friendly forces.

The brigade S3 will ensure that all units operating in and around the brigade support area have taken adequate security measures. These include—

- Ensuring that all units supporting the brigade establish a base defense (villages and towns will assist their defense capability).
- Positioning bases near reserve locations.
- Coordinating with military police to ensure aggressive patrolling and early warning.
- Positioning base clusters to permit observation near critical points, such as bridges or points along main supply routes (MSRs) to observe critical areas.

- Establishing an alert system and communications net for defense of the brigade support area.

The enemy's reliance on communications is extensive for the command and control of attacking maneuver forces and fire support assets, once they are committed to the major battle in the MBA. HPT for ECM resources during this phase in battle include both division-to-regiment and regiment-to-battalion command nets, command observation post (COP)-to-fire direction center (FDC) C^3 facilities, and FDC-to-firing battery communications links.

COMJAM efforts are concentrated against enemy forces conducting or supporting the main attack. ECM operators, targeted against close-in and supporting HPT, maximize the semiautomated capabilities of their COMJAM systems. Other ECM operators are targeted against deeper- and higher-echelon HPTs, such as army-to-division command nets, division-to-battalion skip-echelon nets, and the C^3 facilities supporting the commanders of missile troops and artillery (CMTAs) or army- and front-subordinate artillery and SSM units. They use the full range of capabilities, procedures, and techniques to accomplish their assigned tasks. They selectively jam some HPT using both conventional and special operating techniques. At other times, they may automatically jam these same or other HPT, depending on the HPTs' operational status and the criticality of the information being passed over the given communications links. Unit field SOP and EWTL/JS developed and refined prior to combat and maintained on a dynamic basis as the battle is under way, and special operating instructions and technical data from the TCAE on EW platoons, provide the COMJAM operators the information they need to effectively execute their assigned missions. Direct coordination between the EW team or platoon and the supported maneuver battalion or brigade ensures the synchronization of COMJAM, maneuver, and fire support operations.

Though the maneuver units alternate from offensive to defensive actions, the support units of the brigade must also maintain a constant awareness because they will remain under combat conditions at all times. The illustration on the following page is an example of a BSA.

The battalion combat trains are positioned so close to combat forces that their defense mutually aligns with the security of the battalion they support. Their defense will be addressed in this manual.

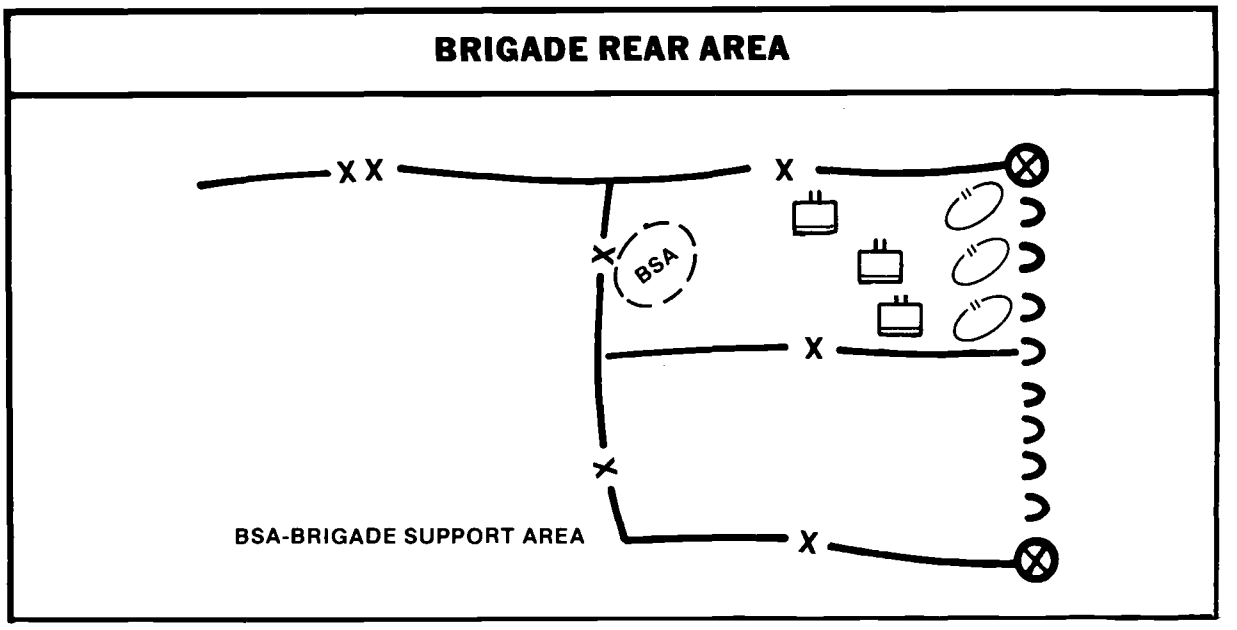
Rear operations will be characterized by intense enemy activity whose intent is to create panic and disruption.

Enemy forces have several objectives in the rear area. These include—

- Destroy nuclear delivery systems, headquarters, logistics, and nuclear storage sites.
- Disrupt C^3, airfield operations, and air defense systems.
- Assassinate high-ranking political and military figures.
- Destroy or seize important LOCs such as highways, bridges, tunnels, and so forth.
- Harass supply lines and troop movements.

The intelligence preparation of the rear operations area is absolutely critical to the success of the air-land battlefield. Besides looking deep and close-in, the intelligence system must also look at the rear operation. To conduct the rear operation successfully, echelon commanders must know enemy capabilities and intentions. They must anticipate enemy actions and receive early warning of incoming incursions in the rear area. This knowledge is obtained through coordination and staff planning by all elements of the brigade staff, especially the S2 and S3.

The BICC, in accordance with S2 guidance, performs the IPB process on the brigade rear operations area in its IPB of the brigade total area of operations. This continuous process develops a comprehensive and accurate data base of weather, enemy, and terrain information from all available sources during hostilities. This information, when integrated and analyzed with other intelligence during hostilities, is the key to determining Level III threat targets, land-



ing sites, and air avenues of approach affecting rear operations. This effort is aided by the various intelligence assets available to respond to brigade tasking.

Besides being familiar with the hostile threat capabilities in the rear area, CI personnel are aware of the scheme of maneuver for friendly deployed units. They know and understand the commander's rear operation plan.

Upgrading intelligence holdings from reports submitted by all sources plays an important part in providing an accurate picture of enemy intentions for the rear operation. Because the rear operation threat is dynamic, CI personnel must continually assess the level of threat and develop and recommend appropriate countermeasures to frustrate or eliminate the Threat.

Incidents of suspected espionage or subversion are investigated by CI personnel as directed. These investigations can lead to identification and elimination of perpetrators of hostile actions in the rear area. Pattern analysis of multiple incidents can reveal enemy plans and intentions.

Identification and neutralization of hostile teams and cells are important priorities in rear operations. Information provided by CI personnel is passed to local police, MP, or allied forces. In a similar manner, these local agencies serve as sources of informs tion in support of CI operations.

Tactical HUMINT operations are employed to exploit those captured personnel who can quickly identify other hostile agents an-d saboteurs and pinpoint unit and team locations, future plans, or weaknesses. Time constraints generally prevent extensive tactical HUMINT operations against level III threats, but enemy agents, sympathizers, and terrorists can often be neutralized at levels I and II.

CI teams located near, or collocated with, the brigade EPW cage will have EPW, refugees, defectors, and line crossers identified by interrogators as being of CI interest. CI personnel conduct interviews or interrogations of these individuals, and are primarily concerned with CI information of current tactical value. Frequently, these interviews or interrogations require a joint effort by CI and interrogation personnel.

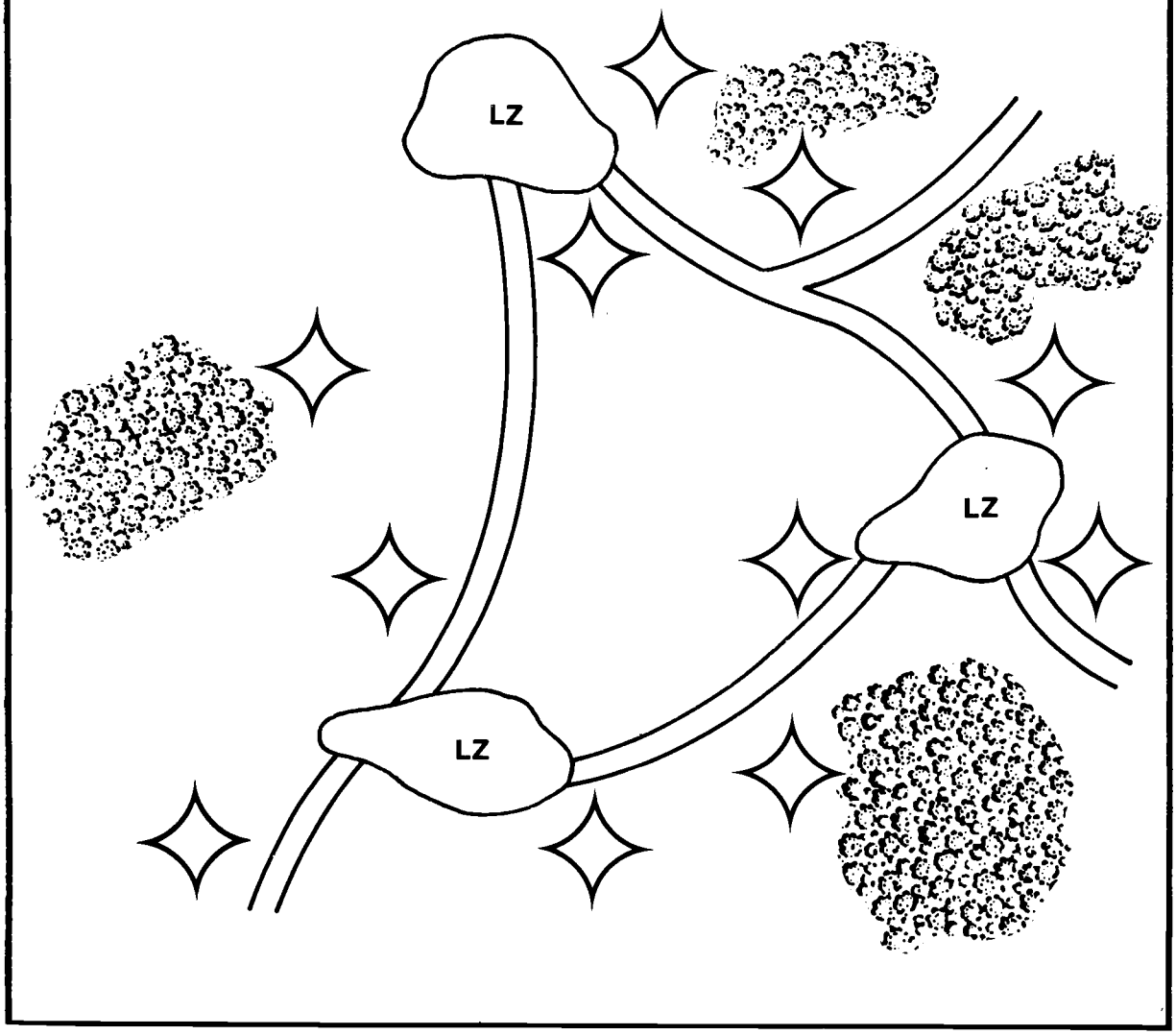
OPSEC support provides the commander with the ability to see his rear operations area through the eyes of the enemy commander. The OPSEC data base is used to evaluate enemy intelligence capabilities and friendly unit high-value targets, patterns, and profiles. OPSEC surveys conducted by OPSEC support teams identify

the vulnerabilities of friendly forces and recommend countermeasures.

COMSEC support teams deploy into the brigade rear area and monitor friendly communications, reporting security violations and unsafe practices to the S2. Enforcement of proper COMSEC procedures denies the enemy critical information through intercept efforts targeted against rear area communications.

When emplaced in likely landing and drop zones, REMS permit rapid identification of enemy heliborne or airborne assault locations as shown below. This applies to small and large insertions of troops behind friendly lines.

LANDING ZONE MONITORING



Sensors may also be extensively used to provide early warning to CSS elements.

The S2, through the IEWSE, may also request ESM support for the rear operation. ESM resources are not generally located in the rear area but may, because of METT-T requirements and the situation, be placed in support of the rear operation. Depending on their availability, resources such as TRAILBLAZER, AN/TRQ-32, or the AN/PRD-10, maybe tasked to intercept and locate enemy radio transmitters in the rear operations area. When there is no SOP for deployment of ESM assets within the rear area, the S3 of the MI battalion will advise the supported element as to the positioning of that resource.

The brigade S3 may request countermeasures to block espionage and saboteur control nets and to jam psychological warfare transmissions and other enemy radio broadcasts. ECM resources in the rear area are also used to isolate enemy special units from their control element's communications. The MI battalion normally retains operational control over all EW assets used in support of rear operations and is responsible for furnishing them with technical data to accomplish their assigned missions.

Retrograde Operations

Retrograde operations are organized movements away from the enemy with the intent of avoiding enemy contact. They are conducted to gain time for the commander to prepare for offensive operations. The primary purpose of retrograde operations is to preserve the force so that, under more favorable conditions, the offense may be resumed. Retrograde operations are also conducted to—

- Harass, exhaust, resist, delay, and otherwise inflict damage on the enemy.
- Draw the enemy into an unfavorable position.
- Allow forces to be used elsewhere.
- Avoid combat when conditions are unfavorable.
- Gain time.
- Reposition forces.
- Shorten LOCs.

The three types of retrograde operations are—

- Delay—trading space for time.
- Withdrawal—disengaging from an enemy in contact.
- Retirement—moving to the rear without enemy contact or pressure.

Because there is no enemy pressure involved during a retirement, no extraordinary IEW operations are required. Normal OPSEC and SIGSEC precautions will be observed.

The IEW principles discussed in the offense and defense both apply to retrograde operations. Commanders require accurate, timely information on which to base their decisions and to execute, at the precise moment, those actions associated with the combat operation.

The commander requires a clear, precise picture of the enemy's disposition, and accurate indications of his intent to conduct operations over the terrain.

IEW resources focus their attention on—

- Locating and tracking enemy forces.
- Determining when and where enemy forces will mass for offensive operations.
- Identifying natural obstacles and key terrain on which the commander plans and conducts his delay in withdrawal operations.

Priority of effort is given to detecting enemy attempts to outflank and isolate friendly forces. IPB will identify routes to enhance friendly force security and mask activities from enemy observation.

IEW support to C^3CM is oriented on destroying or disrupting key enemy C^2 and intelligence links during critical periods of the operation. Especially critical is the period when enemy forces have been stopped and forced to deploy. When this occurs, the delaying force must break contact and withdraw to avoid becoming decisively engaged. Destruction or disruption of key enemy communication links during this

period delays enemy response to the disengagement and withdrawal. This gains additional time for the friendly force to prepare and occupy the next delay position. Simulative electronic deception (SED) is also used to deceive the enemy as to when disengagement has occurred.

OPSEC and deception are essential to the successful conduct of retrograde operations. CI supports OPSEC by assisting the S3 in identifying those critical friendly activities that must be protected to keep the enemy uncertain of their time and place of actual disengagement. IEW systems are used both physically and electronically to deceive the enemy about the disposition of the friendly force. IEW support concentrates those measures that obscure the size and intent of the delaying force and preserve the element of surprise. Each time enemy commanders are engaged by the delaying force they must be convinced through the application of combat power, OPSEC, and deception that they have engaged the main force. This causes them to deploy their forces, reinforce, and prepare to sustain an attack. The delay incurred is the purpose of the delay operation. In addition, the operation creates a situation in which the enemy commanders may expose weaknesses and vulnerabilities that the friendly force can exploit to regain the initiative.

In retrograde operations, centralized control of IEW resources at division level is required. This enables the IEW coordinators to draw upon the full spectrum of the division's IEW assets to achieve the support required for operations.

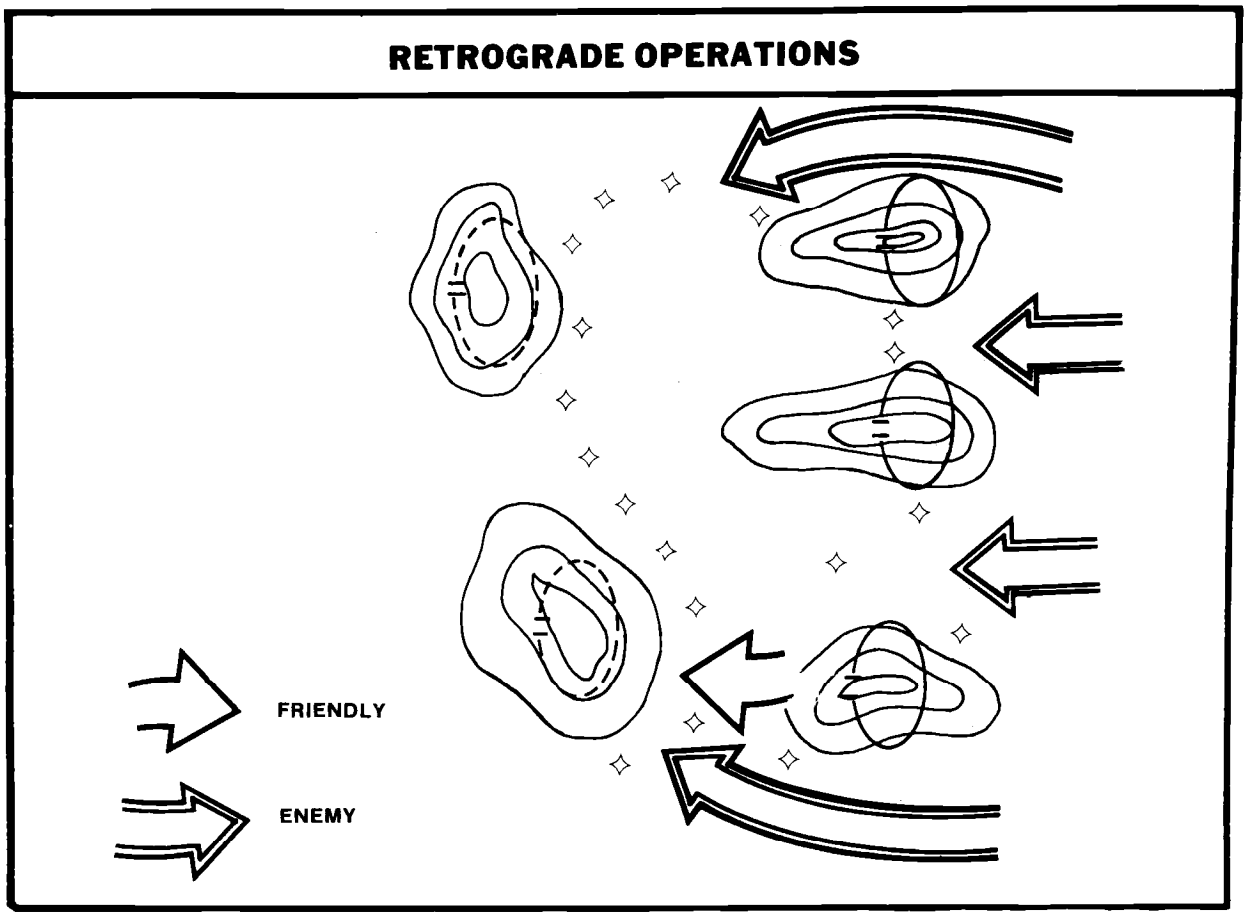
GSR and ESM assets must be deployed well forward to provide maximum coverage for the flanks, any gaps, and for thinly held areas. Support to the brigades must be provided, as well as support to the entire force. To accomplish this, IEW assets must remain flexible and also capable of supporting any follow-on operations.

During retrograde operations, remote sensors may provide an element of security to units conducting the delaying action. Sensors can be emplaced and left in a stay-behind role to provide warnings of when and where enemy forces are moving. Units conducting retrograde may be able to use sensors for flank and rear security. Once the forward echelon of attacking enemy forces has progressed beyond the stay-behind sensors, the sensors will prove valuable by providing indications of resupply or reinforcement activities of enemy rear echelon units. Retrograde operations must be carefully planned in order to locate and install sensor relay equipment. These relays will require camouflage and remote emplacement to avoid detection by enemy forces.

Sensors should also be emplaced in front of the new position to be occupied by our friendly forces. These sensors are employed for several reasons. One reason is to inform the commanders when the friendly units are approaching their new positions. Another application is to offer these units the early warning necessary to continue to avoid decisive engagement. An example of sensor emplacement in retrograde operations is shown in the illustration on the following page.

Delay Operations

In delay operations, a force conducts combat operations designed to retain initiative while relinquishing as little space as possible for as much time as possible. Attack, defend, ambush, screen, raid, and feint make up the delay. There are two basic types of delay techniques under which these operations will fall. These are delay from successive positions and delay from alternate positions. There may be situations in which the commander may want or need to combine the two techniques. The factors of METT-T and the situation will determine the techniques used.



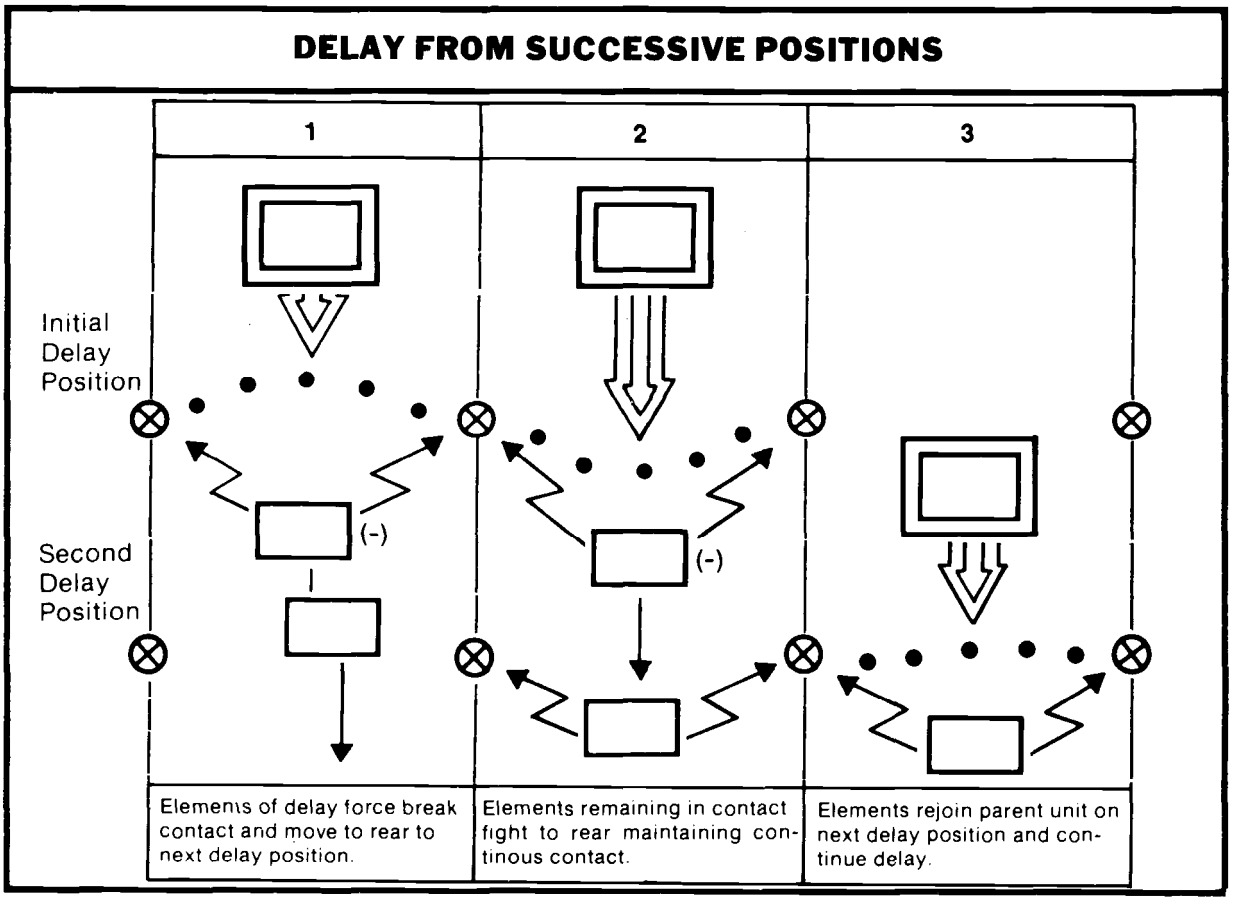
Delay from Successive Positions

This technique is used when the sector is so wide that available forces cannot occupy more than a single tier of positions simultaneously. It requires units to continuously delay in or between positions and is characterized by simplicity of control, minimum preparation of positions, and less depth of forces. It is more easily penetrated than the delay from alternate positions technique. A graphic representation of the delay from successive positions techniques is shown in the illustration on the following page.

This tactic requires that the majority of available forces deploy forward along the most critical sector as determined by IEW resources and, due to the inherent vulnerability to flank penetration, provides major mission support to units conducting an economy of force screen along the flanks. This frees the maximum number of maneuver units for the major avenue of approach, since selection of this tactic presumes a thinly spread force over a wide front.

As discussed in Chapter 4, IPB efforts will identify a series of delay positions that use the natural value of the terrain.

The MI battalion resources are tasked to support brigade and BTF commanders in maintaining contact with the enemy, identifying the enemy's weaknesses, disposition, and intentions. These resources will be located behind the initial delay positions (IDPs) and will focus on first- and second-echelon forces.


DELAY FROM SUCCESSIVE POSITIONS
1
2
3
Initial Delay Position
Second Delay Position
(-)
(-)
Elements of delay force break contact and move to rear to next delay position.
Elements remaining in contact fight to rear maintaining continous contact.
Elements rejoin parent unit on next delay position and continue delay.

CI personnel enhance the force OPSEC posture by ensuring that the IDP, secondary delay-positions (SDPs), and time and routes of withdrawal are concealed from enemy intelligence efforts.

Interrogation assets will not find much activity during this phase of operations, and will assist other IEW functions at the direction of the MI battalion commander.

GSR will be used to survey gaps, critical areas, and avenues of approach, and to obtain target information for long-range fires. They are used primarily for early warning and can furnish significant information about the enemy. The AN/PPS-15, along with other surveillance devices, is used forward of, or on, the IDPs to detect areas of greatest enemy pressure. The information provided will help the commander decide the best time to withdraw to his SDPs. GSRs and other surveillance systems are kept in position as long as possible, both to monitor enemy avenues of approach and to continue the radar emissions to deceive the enemy.

GSR teams in position simulate normal activity, maintain surveillance over the enemy, and move to the SDP prior to the withdrawal of the last maneuver elements left in contact.

EW resources will intercept and locate enemy first-echelon regiment and division communications and noncommunications emitters and perform ECM against enemy high-payoff communications emitters.

Voice collection teams' resources deploy with or behind the maneuver elements' IDPs. Close coordination with the maneuver elements must be established and maintained throughout the operation. Voice collection teams intercept enemy HPTs as determined and tasked by the TCAE. The brigade S2, using PIR and IR of brigade and battalion commanders, requests mission tasking through the IEWSE. The voice collection product will be reported to the

TCAE and concurrently monitored by the IEWSE for information requiring immediate action on the part of the supported commanders. In this instance, combat information will be passed by TACREP to the affected commander through the IEWSE to the S2 or BICC. The technical intelligence is forwarded to the TCAE. Redeployment of the voice collection teams is by order of the next higher commander. Those collection assets located in the SDP will assume coverage of the mission to permit the forward elements' displacement to the SDP. Elements along the flanks between the IDP and SDP will retain their positions until physically relieved and picked up by IDP forces. Upon the completion of occupation of the SDP by IDP elements, those elements originally in the SDP will withdraw to the next delay position.

Throughout the delay operation, EAC aerial assets will provide voice collection targeted against enemy emitters located within the division's deep operations area.

The SPP (TRAILBLAZER) deploys its elements as in the defense. Redeployment uses the same internal leapfrog methods used during both the offense and defense. TRAILBLAZER seeks locations of HPT as tasked by TCAE. Its DF information, together with data from GSR, TEAMPACK, voice collection teams, and other RSTA assets, enable HPTs to be engaged by friendly fire support. Because TRAILBLAZER continuously moves throughout the division area, DF support is less direct than the voice collection support. TRAILBLAZER deploys between the IDP and SDP across the division front, focusing on the expected enemy main effort as determined by METT-T and analysis of the voice collection product. SPP HQ, collocated with one of the MCSs, reports DF results and intercept data to the TCAE which provides information to the brigade S2 via the IEWSE. When the information received by TRAILBLAZER is extremely perishable, the SPP, by TACREP, reports directly to the IEWSE at the affected brigade. TRAILBLAZER redeploys on orders from the MI battalion commander through the TCAE. The leapfrog method is used to retain continuity of the mission. It will be relocated approximately 5-10km behind the SDP and be directed against the main enemy effort.

The noncommunications data produced by TEAMPACK is combined with GSRs, TRAILBLAZER voice collection, and other RSTA assets to assist in targeting for friendly fire support. TEAMPACK is valuable in suppressing and defeating enemy air defense systems, surveillance radars, and countermortar or counterbattery radars by locating them. Identifying the system and plotting its movement provides the commander with the location of the enemy's main effort. Unnetted TEAMPACK reports its data through the EW platoon headquarters to the TCAE, where it is analyzed and reported to the brigade S2. Netted TEAMPACK reports directly to the TCAE and then follows the same route as the unnetted system.

Redeployment of TEAMPACK as the operation progresses is conducted in the same manner as with voice collection resources.

ECM systems are carefully controlled in retrograde operations. Friendly ECM assets are high-priority REC and FS targets and therefore come under the centralized control of the TCAE and division G3. Brigade and battalion commanders will see the ECM systems in their AO but may be unable to task them with the jamming of enemy communications. However, if it becomes necessary to use high-powered communications, because of enemy ECM, the brigade and battalion commanders can task the ECM elements, through the brigade IEWSE, to provide "burn-through" communications capability. Friendly SIGSEC elements can task the ECM elements to conduct COMJAM screening of friendly communications to prevent inadvertent disclosure of sensitive information to the enemy. The MI battalion commander authorizes this ability on orders from the division commander. ECM perform the same function against the same targets as in offense and defense operations. TACJAM will be located in the vicinity of the IDP and TRAFFIC JAM will be located near the SDP. Redeployment of ECM assets is accomplished as is the voice collection team, with the SDP elements assuming the mission for the IDP during relocation. The original SDP elements will

move to other deployment positions toward the rear, once the IDP elements are established in the SDP.

Typical EW element deployment is illustrated in the following figure.

Delay from Alternate Positions

The principal difference between alternate and successive delay operations is that, in the alternate system, two units are used in a single sector. Each delays alternately. While the first is fighting, the second unit occupies the next delay position in depth and prepares to assume delay responsibility. As the first disengages and passes through or around the second unit, the second unit takes up the fight. The first unit then occupies a deeper position and prepares to subsequently resume the delay. Delay from alternate positions is characterized by continuous, more complicated coordination of fire and maneuver, requires more forces, and provides greater security. It is also more difficult to maintain contact with the enemy. A graphic representation of this technique is shown in the illustration on the following page.

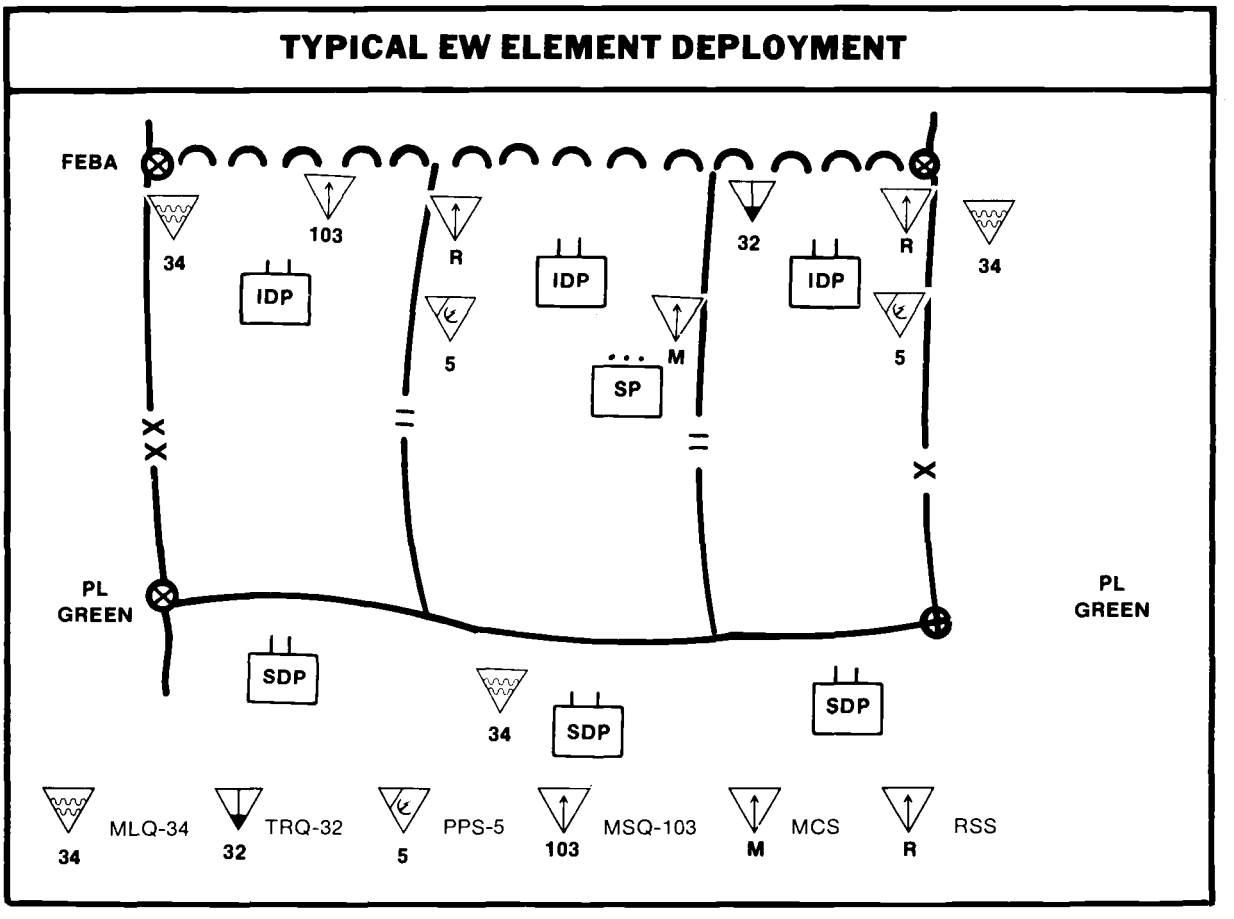
The delay from alternate positions is characterized by a higher density of forces operating on a narrow front.

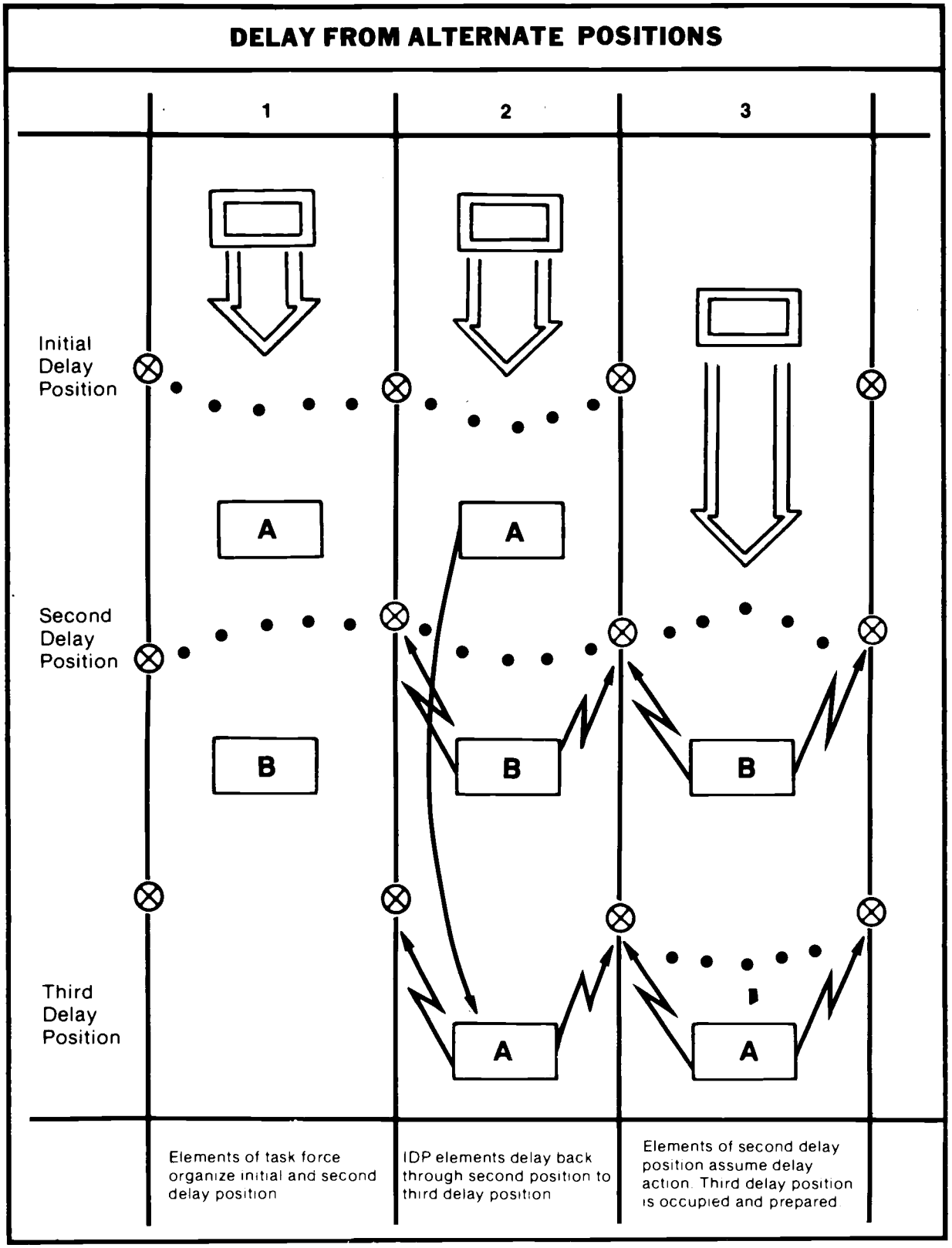
GSR elements are employed in the same manner as during the delay from successive positions, with the exception that those elements organic to Task Force A will remain with Task Force A, while those elements organic to Task Force B stay with their own.

EW elements operate in the same fashion as is accomplished in operations from successive positions.

In all cases, coordination with the maneuver elements is essential.

TYPICAL EW ELEMENT DEPLOYMENT




DELAY FROM ALTERNATE POSITIONS
1
2
3
Initial Delay Position
Second Delay Position
Third Delay Position
A
A
B
B
B
A
A
Elements of task force organize initial and second delay position
IDP elements delay back through second position to third delay position
Elements of second delay position assume delay action. Third delay position is occupied and prepared

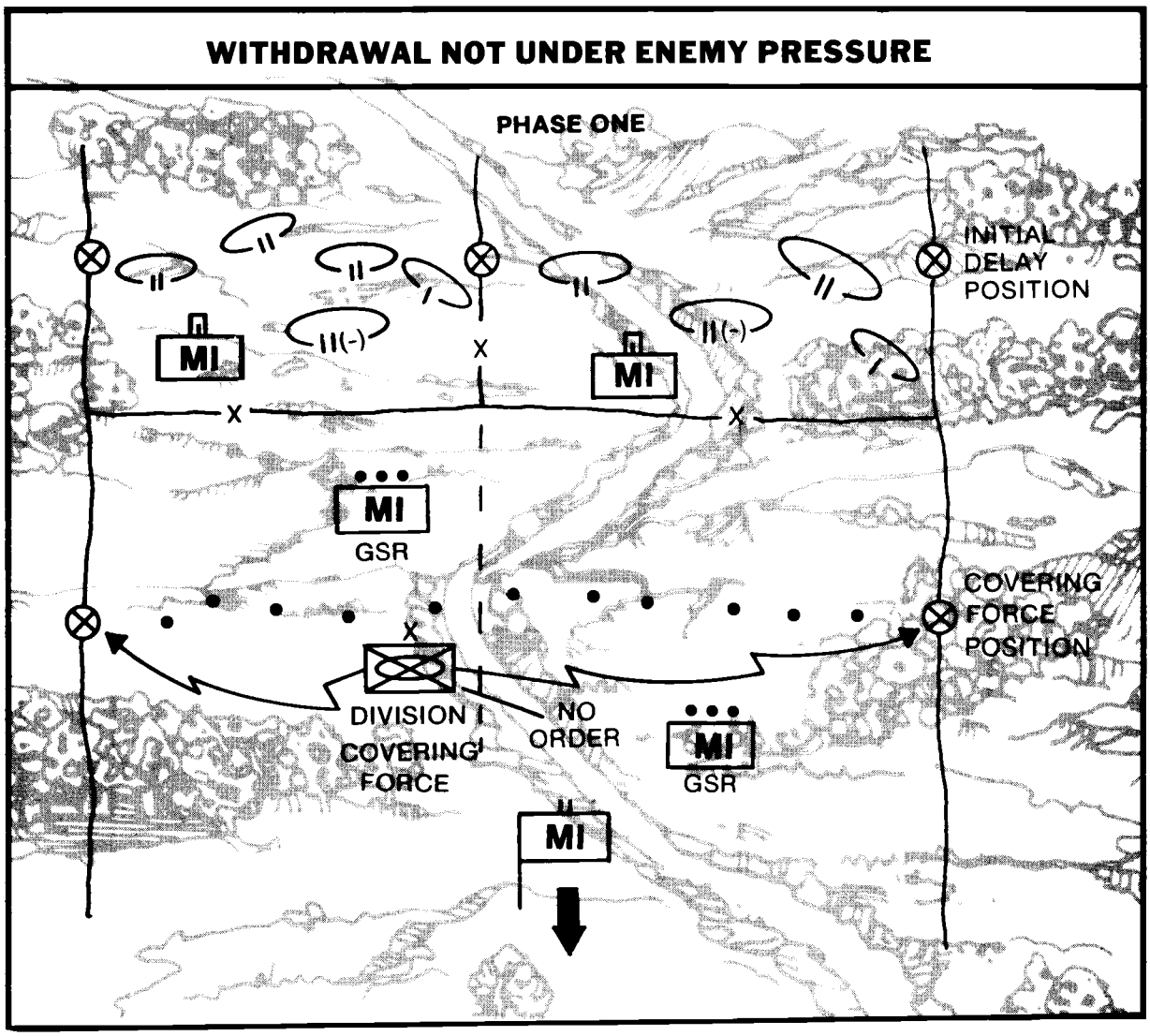
Withdrawal

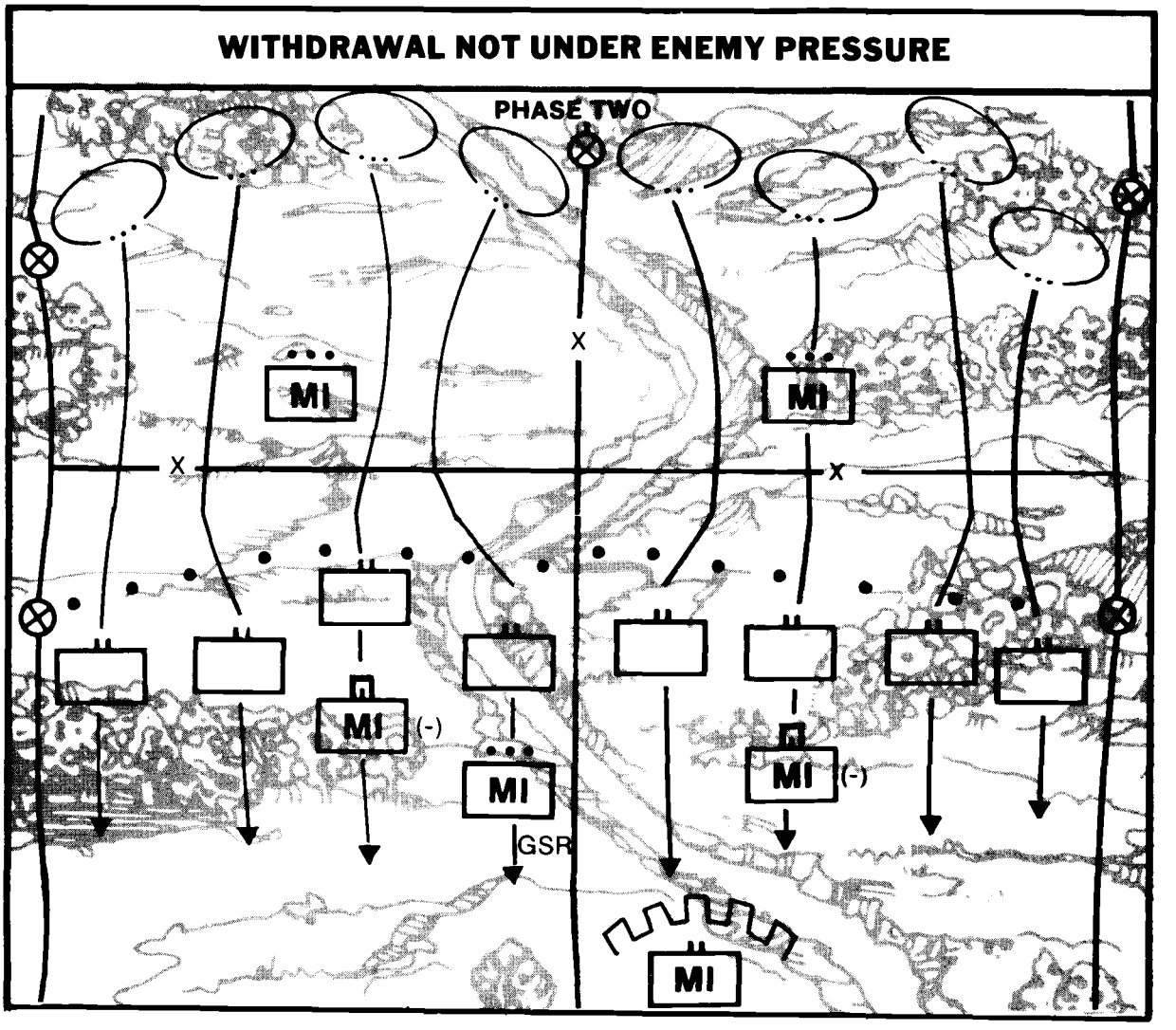
Brigades and battalions assigned a withdrawal mission maintain contact with the enemy to provide security and deception, and to prevent a rapid enemy advance. There are two basic types of withdrawals—

- Withdrawal not under enemy pressure.
- Withdrawal under enemy pressure.

Withdrawal not under enemy pressure affords the commander enhanced freedom to maneuver with minimum casualties. This type of withdrawal is characterized by centralized control and contingency planning, to include alternative routes, priorities, and effective traffic control.

The following diagrams graphically display this technique.





A withdrawal not under enemy pressure operation is begun by the brigade commander designating detachments to be left in contact (DLICs) to protect the initial movement of the main body of the force. DLICs also perform a vital deception role by simulating normal brigade activity, thus masking from enemy intelligence the main body's movement. IEW resources, especially CI teams, play a vital role in this operation.

The simulation of normal unit activity is closely monitored by OPSEC evaluation teams, based on the unit's signatures, patterns, and profiles. In addition to other countermeasures, fire and maneuver are employed to reduce the effectiveness of enemy intelligence collection capabilities. CI personnel assist MP and civil affairs units in maintaining control of the civilian populace in the zone.

GSR elements are deployed as in delay operations and are tasked to observe probable avenues of approach, open areas, and key terrain features, both natural and manmade. In short, they make the enemy believe that the brigade is on line while providing vital information to the DLIC elements.

EW elements will be used in the brigade's CFA, ready to support the operation. All elements not vital to the DLIC withdraw to

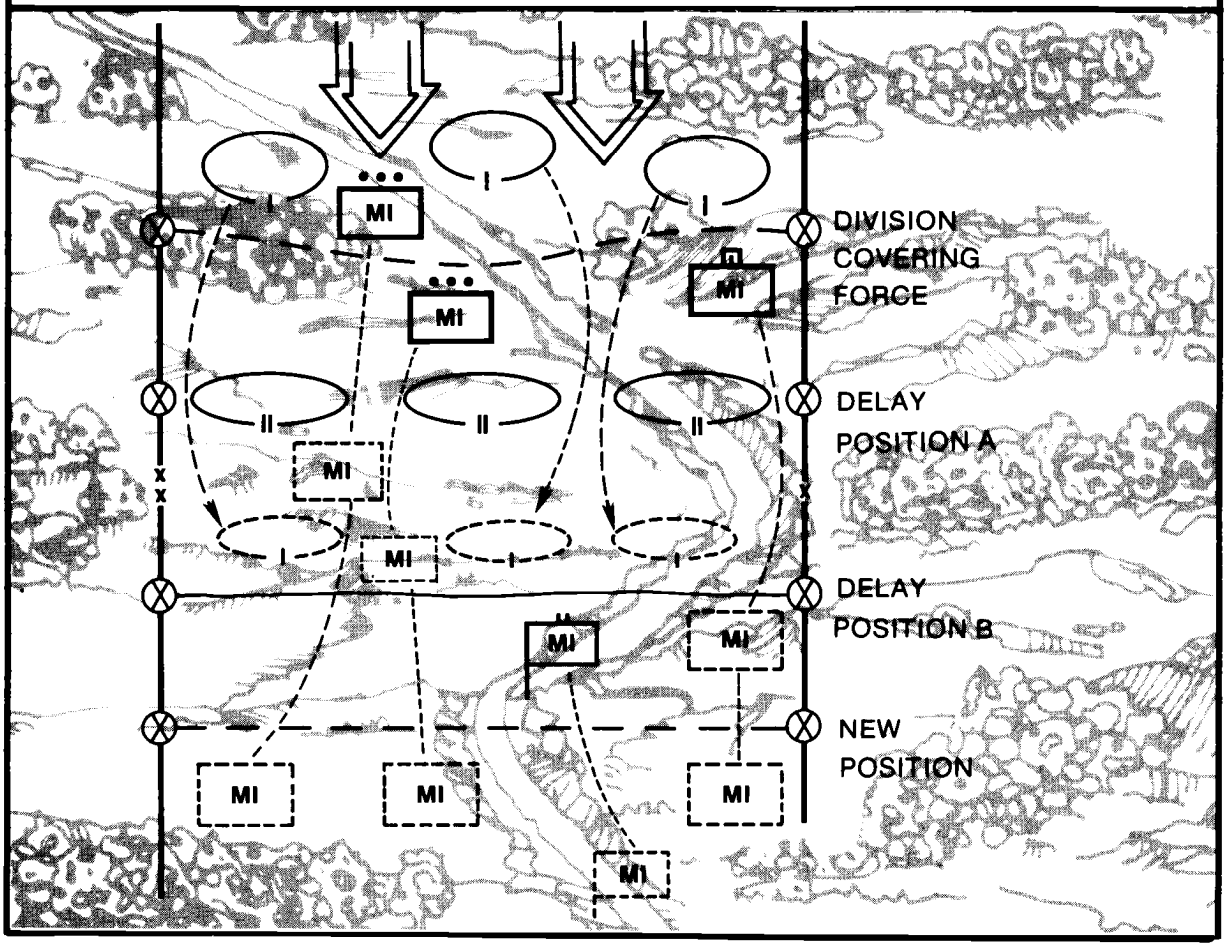
final new positions. The TCAE and the MI battalion support elements are in the first withdrawal. Voice collection, SPP, noncommunications, and some ECM assets will be deployed with the DLIC. Tasking for all EW elements is from the TCAE with a jammer system used to provide high-power VHF "burn-through" communications, if needed. All combat information and perishable intelligence will be reported to the brigade S2 through the IEWSE and all technical intelligence will be routed to the TCAE through the SPP when communications allow.

All MI assets with the DLIC will deploy to new positions through the covering force when the DLIC withdraws. GSR assets assist to vector the DLIC during periods of poor visibility and darkness.

Withdrawal under pressure differs significantly from withdrawal without pressure. Units use delaying tactics to fight their way to the rear. All units initiate action simultaneously in a given sector. A covering force is highly desirable to assist the disengagement of committed units. It may also be used to initiate a counterattack. Key to the successful conduct of a withdrawal under enemy pressure is superior mobility, effective covering force employment, sound C^2, and local air superiority. A graphic example of a withdrawal under pressure is shown below.

IEW support and actions are similar to a delay from alternate positions.

WITHDRAWAL UNDER ENEMY PRESSURE



OTHER TACTICAL SITUATIONS

Defense and Breakout of Encircled Forces

The nonlinear nature of the modern battlefield presents units with a high probability that enemy forces will encircle them. This is especially true at the brigade and BTF and of the MI elements supporting them. Encirclement of friendly forces may happen by a rapidly changing situation or may be by design.

Defense

When encirclement is unforeseen, the first action to be accomplished is that the senior commander present must organize a defense and establish a unity of command. The most immediate problem facing the commander is the preservation of the force. Breakout from the encirclement is the next priority. If a breakout is to be made, the attempt must occur before the enemy can consolidate their positions. If no breakout attempt can be made, the, commander continues the defense and plans for a linkup and to assist a relieving force. The commander must reorganize and consolidate the units within the encirclement to include the IEW assets and MI units.

IEW support to the encircled forces is vital. The force commander must receive intelligence immediately concerning the following:

- ☐ Composition and disposition of encircling enemy force.
- ☐ Enemy reinforcement units.
- ☐ Exploitable weaknesses in the enemy disposition through which breakout or linkup can be effected.
- ☐ Enemy intent to use NBC weapons.

ECM support is crucial to the breakout and deception operations.

The following chart depicts the tasks that the commander must accomplish and what the S2 and senior MI commander must do to support those tasks.

IEW SUPPORT TO DEFENDING ENCIRCLED FORCE

ENCIRCLED FORCE COMMANDER	IEW SUPPORT
Re-establishes chain of command	• MI chain of command established • Re-establishes communications with higher (parent) MI unit
Establishes a viable defense	• Orients on the dangerous avenue of approach • Disperses and protects IEW systems for survivability • Integrates MI elements into defensive plan
Establishes a reserve	• Assigns MI elements on-order missions to support commitment of reserves to contain penetrations/maintenance of interior lines
Reorganizes fire support	• Establishes procedures for integration of EW
Reorganizes force logistics	• Centralizes common supplies • Enforces supply discipline • Acquires external SIGINT/EW/GSR unique resupply if required, possibly by air drop or helicopter lift
Establishes security	• Integrates IEW assets • Provides CI support

While part of an encircled force, MI elements respond directly to that force commander's requirements. The senior S2 of the force will establish the HVT and HPT for the MI units based on the previous chart and METT-T. The efforts of the MI elements of the encircled force must be coordinated with efforts of those MI elements at the main force outside the encirclement. Use of high powered jammers could be required to provide "burn-through" communications for this coordination because of heavy enemy COMJAM operations.

The senior MI commander assumes temporary C^2 over the MI elements within the encircled force. That officer is responsible for the quick reorganization of the MI elements available to the force commander. That reorganized MI unit will then respond to the commander as the divisional MI battalion does.

EPWs are interrogated by available EPW interrogation teams to ascertain the size of the enemy force and its strengths and weaknesses, to include personnel and equipment makeup. Information as to the size, location, and availability of enemy reserve forces is also obtained.

GSR teams are deployed around the encircled force to provide the S2 and force commander with information on locations and size of enemy front-line forces, and to provide early warning about enemy movement to attack. GSRs are also used to vector patrols through enemy front lines during probing actions.

EW elements deploy, are employed, and redeploy similarly to the delay from successive positions in retrograde operations.

All tasking for the ESM elements is from a reorganized TCAE or analysis section based on the force commander's priority and target list as outlined in Chapter 4. Primary targets will include enemy forces' disposition and any reinforcing elements. Reported combat information goes directly to the force commander through the IEWSE and S2. Any technical data will be reported to the analysis section of the reorganized TCAE as time and the situation permit. SPP (TRAILBLAZER) elements in the encircled force area will respond to tasking as will other voice collection assets. Target locations are unlikely, so the SPP elements that are available will provide communications intelligence and LOB data. The SPP headquarters element, if in the encircled force area, becomes the primary element in technical control and analysis for the encircled EW elements if there is no other TCAE present. The MCS, if present, will be used as the primary intercept and LOB station, due to its accuracy and sensitivity above the AN/TRQ-32 and MRDFS elements. The RSS elements are used as LOB data stations. All ESM elements are employed within 2 to 5 kilometers of the FLOT as directed by the MI commander based on the force commander's priorities.

Noncommunications intercept elements (TEAMPACK) will be used primarily to locate the enemy fire support radar systems, GSR systems, and air defense radar systems. This enables the S2 to determine the enemy's main effort and troop concentration. Intelligence from TEAMPACK is reported to the S2 through the IEWSE. All technical intelligence is transmitted to the designated TCAE as time and situation permit. As with TRAILBLAZER, TEAMPACK will most likely be separated so that only one or two units will be available to the MI unit commander for tasking. Precise locations of the enemy radar systems will be impossible using the separated TEAMPACK element, but LOB data will be available. Using this, along with other ESM data, GSR results, OP observations, and friendly countermortar and counterbattery radar results, an accurate location can be determined.

ECM assets have, as stated previously, the number one priority of providing the force commander with a high-powered communication capability that allows for continuous coordination with the main force. If the commander requires a deception operation, C—E and CI assets provide a vital element for SED operations. COMJAM equipment can be used for demonstration and feints. Deployment of COMJAM systems is dependent upon specific mission requirements. Because of heavy enemy REC activity, the TACJAM and TRAFFIC JAM systems must redeploy, often away from

any friendly C^2 elements. All ECM assets in the encircled force are tasked by the MI unit commander to attack HPT, based on the force commander's priority. Tasking is accomplished through the EWO and the supported staff element.

All IEW elements are prepared to support breakout and linkup operations. The attack to break out of an encirclement is conducted on a narrow front, while a simultaneous defense is conducted in the remaining sectors of the perimeter. The encircled force is organized into four elements for the breakout:

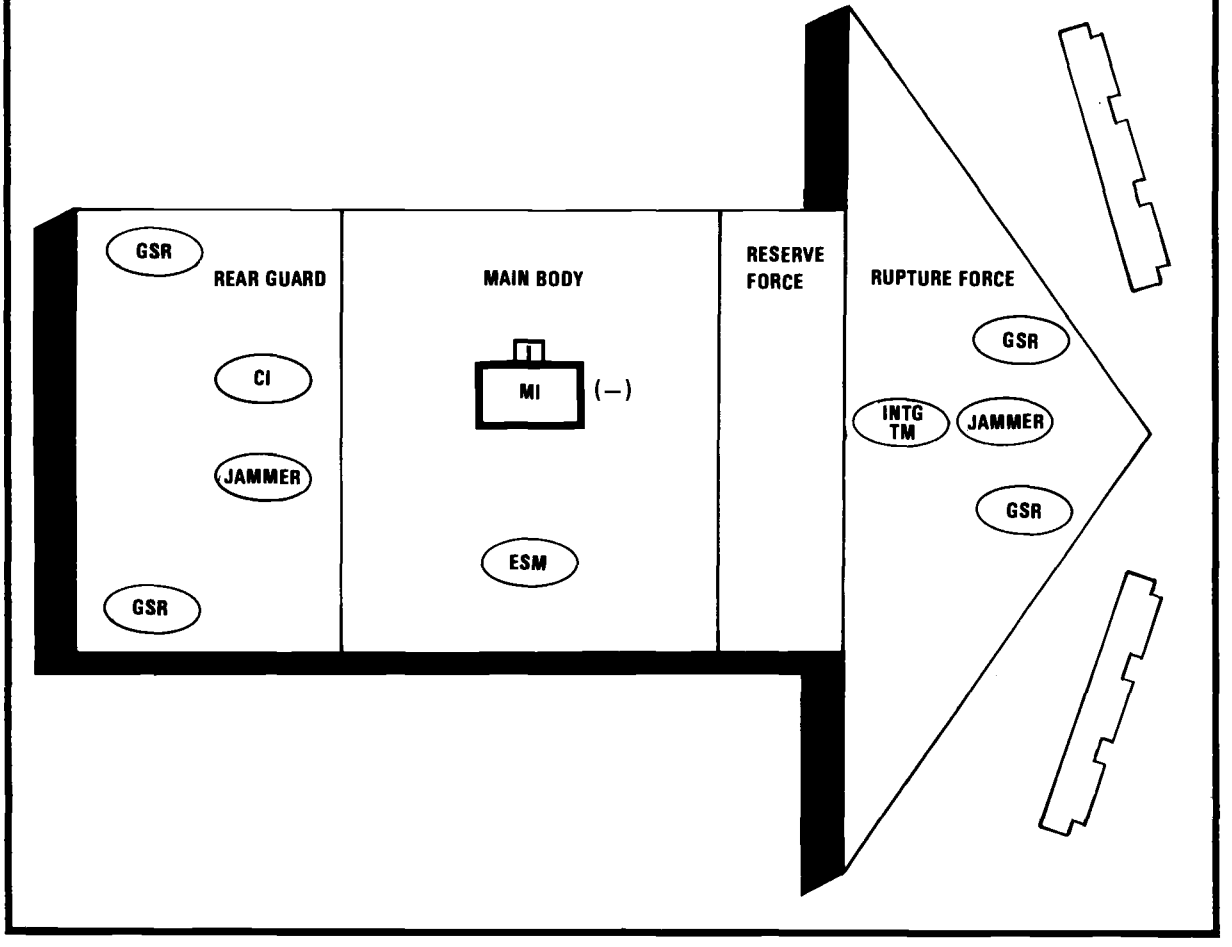
- Rupture force.
- Reserve force.
- Main body.
- Rear guard.

The force commander, as with defense of the encircled force, has certain tasks he must perform to accomplish the breakout. The chart on the following page shows the commander's tasks and the applicable IEW support measures for those tasks.

The following figure portrays the breakout force and possible IEW resource disposition within that force.

The rupture force opens the gap that the rest of the breakout force will pass through. It holds the shoulders until the main body passes through and is joined by the rear

THE BREAKOUT FORCE



IEW SUPPORT TO PREPARATIONS FOR BREAKOUT

ENCIRCLED FORCE COMMANDER	IEW SUPPORT	
Deceives the enemy as to the time and place of breakout	• Advises and assists in preparation of plan to include OPSEC aspects	• Provides CI and ECM support
Exploits gaps and weaknesses in enemy forces	• Identifies enemy dispositions and possible reinforcements • Identifies exploitable advantages of weather and terrain; especially concealed routes • Directs collection to fulfill information gaps	• Identifies assailable weaknesses
Exploits darkness and limited visibility	• Uses GSR to vector forces	• Uses GSR for targeting
Organizes the breakout force	• Integrates MI support into advance force, main body, and rear guard • Integrates ECM into breakout to magnify surprise, enhance shock effect, and "freeze" enemy in place • Sees ahead of advance force to maintain momentum to breakout • Provides combat information to unit conducting supporting attack	• Ensures continuity of IEW communications via aerial relay during breakout • Uses ECM to "slow/freeze" enemy reinforcements • Jams fire control communications • Provides surveillance and reconnaissance for flanks and rear • Coordinates coverage with higher IEW staff/unit • Provides CI support
Re-establishes communications	• Reports all deep operations data to higher headquarters	• Requests aerial/ground relays
Limits damage by nuclear or chemical attack	• Increases MOPP level • Locates and reports enemy NBC delivery systems	• Ensures NBC readiness • Takes action to minimize effects of EMP
Continues the defense	• Develops contingency plans	• Provides continuous IEW support
Maintains morale	• Counters rumors, subversion, sedition, and propaganda	• Jams enemy PSYOP intrusions
Considers exfiltration	• Develops intelligence reporting channels to exploit HUMINT in the breakout corridor • Provides CI coverage for evacuated areas and CPs	• Provides counter-technical intelligence for destroyed equipment • Provides wounded with EEFI • Supports creation of diversions

guard. As shown on page 5-57, the armor-heavy rupture force will use GSR, usually the high-powered AN/PPS-5 to vector away from enemy force concentrations or during periods of low visibility or darkness. The EPW element screens any prisoners or documents acquired during the rupture force breakout. The information gathered is sent to the encircled force commander through the S2 at the main body. EW elements consist solely of jammers. The jammers disrupt enemy C^2 to both maneuver and fire support elements near the breakout area. The MI command element, with the main body, will task and control the rupture force jammers based on ESM and GSR collection efforts.

The reserve force does not possess any IEW resources until it assumes the role of lead element to the breakout. The rupture force holds the flanks to allow the remaining forces to break out. When the reserve force passes through the rupture force, it assumes the rupture force IEW assets. The GSR, EPW, and ECM elements continue to perform the same functions and are tasked and respond the same way as when attached to the rupture force.

The main body consists of the encircled force commander, his headquarters, and remaining combat support and CSS elements. The MI units' headquarters analysis element and all ESM elements move with the main body. From this area, the ESM assets can cover the rupture and reserve force, flanks, and rear guard area. The MI headquarters assists the force S2 and commander in controlling all the MI assets.

The rear guard provides the deception effort to confuse the enemy as to where the main effort is to occur, and provides protection to the rear of the force as it progresses through the rupture. The rear guard is usually placed under the control of the force XO, and contains a representative force structure to simulate the main body. The rear guard acts as a covering force. CI elements provide for OPSEC and prevent disabled equipment, supplies, and CPs from falling into enemy hands. GSR elements provide flank and rear security and targeting data for FSE. The ECM assets will disrupt the enemy's C^2 and slow down any reinforcement.

Once the breakout is accomplished, the force commander re-forms the force into movement to contact configuration, as described earlier in this chapter. Every effort is made to bypass enemy forces along the route. If bypass is not possible, the force will move to the hasty attack from the movement to contact mode.

If a breakout is not possible, relief by another friendly force is probable. The relief force attacks the encircling enemy force's rear area and defeats him. The encircled force commander and IEW assets perform the tasks outlined in the chart on the following page.

Heavy enemy REC is expected in this phase of operations. ECM assets will provide high-powered communications among the encircled force commander, relief force commander, encircled MI element commander, and MI commander attached to the relief unit. ESM elements will operate as in defense operations.

GSRs provide the relief force commander with probable avenues of approach, and assist in vectoring the relief force during periods of darkness and low visibility.

IEW SUPPORT TO LINK-UP OPERATIONS	
ENCIRCLED FORCE COMMANDER	**IEW SUPPORT**
Coordinates plans for linkup	• Shifts IEW control to linkup force • Exchanges enemy situation data • Coordinates and fulfills PIR • Provides IEW-unique logistic requirements • Sees deep and develops situation for actions after linkup • Receives IEW liaison officer • Coordinates CEOI for IEW
Supports the relief attack	• Reads battle and reports to relief force • Supports with ECM
Coordinates subsequent actions	• Coordinates subsequent actions

SPECIAL OPERATIONS AND ENVIRONMENTS

The geographic range of US interests in the world today requires that the Army be prepared to fight and win in all types of terrain and climate.

Army tactical units may be committed to battle in those areas where severe weather, climate, and terrain impact on military operations and the intelligence mission. In addition to the physical effects on the individual soldier, environmental extremes limit intelligence collection capabilities. Regardless of environmental conditions, the commander needs information about the enemy, weather, and terrain.

Special operations are those in which the natural and man-made characteristics of the area, the nature of the operations, and the unique conditions under which the operations are conducted, may require specially trained personnel and special techniques, tactics, or equipment.

The environments that have a strong effect on special operations are—

- ☐ Mountains.
- ☐ Jungles.
- ☐ Deserts.
- ☐ Winter.
- ☐ Urbanized terrain.

While the fundamental principles discussed in previous chapters apply to special environments, brigade and battalion S2 personnel must understand the limitations imposed on collection resources by harsh environments. Specialized training and acclimatization periods are required before personnel can be effective in certain parts of the world.

The effects of extreme climatic and terrain factors generally cause military operations to proceed at a slower rate than in more favorable environments. Set-up and break-down times may be longer, and rates of march slower. Routine functions, such as communications, can become a major

undertaking. S2s ensure that intelligence planning for combat operations takes into consideration the influence of a special environment on intelligence functions, personnel, and friendly and enemy operations.

While the means to collect data in special environments are identical to those employed in a normal environment, the methods of employment and equipment used may differ.

The enemy's methods of employment and deployment will also differ, but only to the extent permitted by their doctrine, or dictated by the environment.

MOUNTAIN OPERATIONS

Mountainous terrain exists in the jungle, temperate, and arctic regions of the world. Operations conducted in mountainous areas are characterized by heavy use of indirect fires, canalized movements along valley floors, decentralized combat, increased collection operations from aerial IEW operations, and reduced C^2 capabilities. Mountain operations conducted by MI units have restricted operational and sustainment capabilities.

Mountainous terrain degrades target acquisition and early warning capability of GSRs, and collection capabilities of EW systems. Such degradation places an increased importance on emplacement and utilization of GSR and EW systems. Both elements may have to use their manpack equipment to best support the commander.

Because of the low density of manpack IEW equipment in the division, brigade areas will be unsupported or severely reduced in GSR and EW support. Although operations may be severely hampered, the mission for all MI assets remains the same as in any other type of operation. The optimum operation of these IEW systems in mountainous terrain is affected by interrupted LOS, extreme temperature variations, heavy precipitation, and a lack of readily available support and supply parts.

In mountain operations, the terrain isolation of friendly units may require brigades and battalions to operate more independently than in other environments. In this case, the S2 is required to make judgments beyond the scope of his usual role. S2s may find themselves unable to communicate with higher and adjacent units, forcing them to rely on their own resources to develop intelligence and determine an enemy's probable course of action.

Mountain weather is difficult to predict. In many areas, the weather can change dramatically in short periods of time. As storms develop, the effects of the temperature and windchill factor may become as important an item of intelligence as the location and activity of major enemy units. Exposed flesh can freeze in a matter of seconds. The higher elevations are frequently shrouded by rain, snow, sleet, and fog. Electronic surveillance and visual observation are severely limited under these conditions.

When weather permits, mountain heights offer outstanding conditions for long-range visual observation and electronic surveillance.

Weather data and forecasts are increasingly more important in selecting areas and times to conduct operations.

Cross-country movement and trafficability become more important in determining enemy capabilities and intentions. Potential enemy use of nuclear weapons in mountainous terrain is a prime intelligence consideration. In some mountainous terrain, the effects of nuclear detonation can be effectively contained within a specified area.

Wooded mountainous terrain has the same general effect on intelligence operations as does dense jungle. Enemy forces are difficult to locate and collect against. As in jungle terrain, the S2 will find his best sources of information to be EPW, defectors, and friendly reconnaissance patrols.

Mountainous terrain favors those operations which use stealth and the cover of darkness. Forces will likely be deployed to control passes, road junctions, built-up areas, and the high ground adjacent to these areas. Enemy tactics include bypassing defensive positions and attacking from the flanks and rear. Enemy forces will decentralize the employment of artillery

and use multiple rocket launchers as individual fire units.

S2s rely on front-line soldiers, aircraft crews, vehicle operators, and maps for terrain analysis.

Mountain tactics favor the use of helicopters to drop enemy forces behind friendly emplacements, and for reconnaissance, C^2, resupply, and evacuation.

Enemy forces can be expected to use infantry troops in the higher elevations. Motorized rifle units and tanks may be encountered in the lower elevations, broad valleys, depressions, and on the slopes of small hills.

In defensive positions, enemy tanks will be found in tiers on both forward and reverse slopes, usually within platoon-sized strongpoints. Enemy defensive frontages can be expected to increase in mountain warfare. The enemy force will select the terrain most suitable for defense and the most inaccessible to the friendly force. Mountain operations are usually directed at the control of passes. The force that controls the mountain passes controls a significant amount of terrain.

Rugged, irregular mountain terrain degrades AM and FM communications effectiveness and associated C^2. Heavy reliance on retransmission and relay is required. Heavy (TACJAM) and medium (TRAFFIC JAM) ECM equipment can be used to relay communications when necessary.

HUMINT provides the commander with his best source of combat information and intelligence. Mountain heights offer exceptional OP sites which may be supplemented by foot patrols. Population centers in valley areas provide a HUMINT collection and interrogation potential, especially for terrain intelligence information.

OPSEC, as in all operations, will be of prime importance for attacking forces. Defending forces will have a distinct advantage to deceive and contain any attack.

EW operations suffer a definite disadvantage in mountainous terrain. Enemy communication sites use terrain masking, relay, and retransmission to thwart both RDF and ECM activities.

The irregular terrain, multitude of dead spaces, and degraded C^2 will render EW less effective in the mountains than in other types of terrain.

ESM systems, such as TRAILBLAZER and TEAMPACK, are best employed on high ground, concentrating on enemy approaches.

ECM systems will find the most effective use in the same area as the ESM assets. Their employment is directed against the population centers, enemy broadcast blocking, and avenues of approach. ECM equipment (TRAFFIC JAM) is also used to retransmit friendly C^2 messages.

Aerial systems, SLAR and QUICKFIX, are used in other operations, although the mountainous altitude may require the QUICKFIX crew to use oxygen and operate for a shorter duration.

Ground-based RDF is accomplished by the MRDFS often employed in DS to the brigades. The amount of support provided will depend on equipment density. LOB data may be questionable, due to the terrain, but will normally be used in conjunction with QUICKFIX.

Sustainment considerations in special operational environments can be numerous. Equipment used in a mountainous environment must be rugged and man-portable. Cold weather in the higher elevations, or during seasonal variations, will affect equipment in the same manner as in winter operations.

Transportation limitations will require greater use of field expedients than in other types of operations. Because of the rugged nature of the terrain, greater consumption of Class IX repair parts will occur, and will demand a 20 percent overage in PLL and ASL for such items as tires, transmissions, clutch plates, filters, brake shoes, tracks, track pads, and fuel pumps.

The key to sustaining soldiers in the mountains, as in other special environments, is training. Mountain combat can affect a soldier's mental alertness, accentuate fears of heights and closeness, and cause dehydration and sickness.

Additional information on mountain operations is contained in FM 90-6.

JUNGLE OPERATIONS

The jungle regions of Asia, Africa, and Central and South America are potential areas of conflict where US forces could be involved. Jungles vary from tropical rain forests and secondary growth to swamps and tropical savannas. Heavy rainfall, high and constant temperature, high humidity, and thick vegetation are the dominant features of jungle areas. These factors—climate and vegetation—contribute to the restriction of operational and sustainment capabilities of MI units.

Because of the nature of the jungle, IEW operations will be decentralized. Ground mobility restrictions of the jungle require that all IEW systems be light, man-portable and rugged, and fielded in greater densities than in other, more open environments.

The climate, dense vegetation, and subsequent reduced radio LOS, significantly reduces communications in both AM and FM. Electromagnetic radiation is absorbed by a factor of 10 to 25 percent and communication ranges will decrease by a factor of 20 percent. To facilitate effective C^2, hilltops or aerial relays may often be used. Although wire appears a logical method, security and maintenance considerations may preclude its use.

Jungle vegetation limits identification of sounds, smells, deployments, movements, locations, and other activities which might otherwise be detected. It severely limits the use of enemy force signatures to identify types of units and activities. Intense tropical storms can temporarily preclude the use of electronic collection equipment. Thick jungle terrain restricts mobility largely to roads and footpaths. The S2 may find that the best sources of information are EPWs, defectors, patrols, and the local populace—in other words, HUMINT.

The local populace can provide a wealth of information about enemy forces operating in the local area. In insurgency situations, efforts are made to identify individuals that support the enemy by providing supplies, food, and information about friendly forces in the area.

Heavy rain showers limit the detection of enemy electronic signatures to short ranges. GSRs in heavy jungle foliage will be of little or no value. Signal reflections from vehicles and troops passing through or behind dense foliage tend to be inaccurate and unreadable. Although GSR operations in jungle environments normally are limited, they are still a valuable asset to the supported commander when properly employed. GSR is particularly useful in preventing surprise when used with other battlefield surveillance devices. REMS located along roads and trails indicate activity on those routes, but cannot distinguish between enemy and other activity.

Lightly equipped LRRPs and long-range surveillance units (LRSUs) play a major role in jungle intelligence collection operations. The terrain improves chances for accomplishing their mission unobserved and undetected. In patrol planning, consideration is given to the possibility that an aerial resupply, often required in jungle operations, will provide the enemy with indications of patrol activity and possibly reveal the location of the patrol. Communications are also a problem. The intelligence value of the reconnaissance is reduced if intelligence and targeting data is not rapidly communicated.

The limitations discussed in Chapter 2 for the EW systems are heightened by the jungle environment. ESM ground systems are located in various base camps throughout the division's AO, concentrated in the brigade where the expected enemy main effort will occur.

ESM systems, to include TRAILBLAZER and TEAMPACK, may be used more as individual collection stations than as integrated systems, due to the environment.

The lightweight, highly mobile systems, such as the MRDFS, will find extensive use. Deployment will be with patrols—foot or mounted. The MRDFS provides intercept and LOB data to the patrol leader and TCAE.

The divisional aerial assets provide the best means of intelligence operations for IEW elements. The supporting corps SLAR aircraft, in conduction with GSR and

REMS, present the commanders with the best picture of the battlefield. The QUICKFIX provides excellent radio LOS to all targets for LOB, intercept, and COMJAM operations. The TCAE, based on IPB and the brigade's needs, tasks and controls the aerial assets. High incidence of rust, corrosion, and fungus, caused by jungle moisture and humidity, highlights the necessity for daily maintenance on equipment—especially at the operator level. This is especially true for electronic systems and COMSEC gear, which are subject to very high failure rates in jungle environments. Continuous operation of such systems generates heat, which combats moisture, corrosion, rust, and fungus, decreasing the mean time between failures, but hastening system wearout.

Mountainous regions may also be found in jungle areas. These areas are particular difficult for patrols to traverse, especially during the rainy season. In these regions the extremes of weather can run from very hot and humid at the lower elevations; to cold and wet at the highest elevations.

DESERT OPERATIONS

The use of IEW assets in desert operations demands special preparation in order to conduct combat operations.

Deserts are semiarid regions containing a wide variety of soils in varying relief. There are three types of desert: mountain, rocky plateau, and sandy or dune. Optimum operation of EW equipment in desert terrain is affected by dust, sand, temperature variations, static electricity, and wind.

Desert operations are characterized by the use of forces that are capable of conducting highly mobile operations. These operations significantly increase the size of the area of interest at virtually all echelons. Collection assets are focused on targets at significantly greater distances than normal. Brigades and battalions may become even more dependent upon the division and corps for intelligence, because collection requirements may exceed the range of their collection capability. This requires more DS and GS reinforcing missions. The mobility factor of the desert requires more tracked and fewer wheeled vehicles for EW systems.

The desert battle is highly mobile. An attack may be carried out from the line of march. Enemy battalions deploy to company columns 12 to 15 kilometers, and platoon columns at 3 to 5 kilometers from the assault position. Enemy doctrine dictates that tank formations will generally be used in the first echelon, and that the attack may be conducted using a single echelon. The enemy may employ airborne and helicopter assaults to seize objectives in the rear.

Frequent and extreme changes in desert weather have a significant influence on intelligence collection capabilities. Long periods of unlimited visibility are abruptly interrupted by violent winds and sandstorms. These storms reduce visibility and drive sand into mechanical and electronic equipment, causing frequent breakdowns.

The wear and tear, particularly on mechanical equipment, requires frequent replacement of moving parts. Increased requirements for spare parts place an additional burden on the supply system, increasing the vulnerability of friendly logistic operations. Wide variations in day and night temperatures also have detrimental effects on people and machines. Precautions must be taken to prevent casualties resulting from direct exposure to the sun and high temperatures.

The high desert temperatures may cause equipment to overheat. Heat causes batteries to lose power more quickly. High temperatures cause overheating in communications equipment resulting in equipment failure. Lenses on DODs can become discolored when directly expose to sun. Communications equipment must be protected from heat and from the direct ray of the sun.

Degradation of AM and FM radio communications occurs due to extreme heat. Communications during hours of darkness are excellent. During daylight, a 20- to 30-percent loss of radio communications is experienced, due to heat. Frequency drift will also limit radio capabilities.

EW systems and radioteletype equipment will also suffer frequent down time from sand and dust, if not protected. IMINT systems are subject to heat wave distortion and

dust storms. HUMINT operations are reduced, due to smaller population areas. OPSEC responsibilities increase significantly due to the long range of enemy IMINT and SIGINT systems in the desert. Like OPSEC, the value of EW has increased in importance. The expansiveness of the desert precludes using terrain masking to avoid jamming. ECM can freeze the battle for destruction by fire and maneuver, and plays a significant role in air defense and CAS suppression.

Vehicle maintenance requirements increase in extreme heat. The heat dries out seals and gaskets and causes tires to crack. The effects of sand on equipment creates the need to constantly replace bearings and other moving parts. Since reconnaissance in desert operations is generally accomplished using mobile patrols, maintenance requirements will directly impact on reconnaissance capabilities.

Humidity and temperature variations cause condensation and rust. Condensation degrades the effectiveness of the optical devices by causing mold to form on lenses, requiring extra precautions to be taken. Equipment must be cleaned on a daily basis. The problems associated with desert observations and reconnaissance include—

- Long ranges and the refraction of visible light impairing visual perception.
- Heat waves, blurring detail.
- The actual location of observed objects becoming difficult to determine.
- Mirages, which can distort objects to the point of being unrecognizable.

The intensity of these effects often depends on the angle of the sun in relationship to the observer. Observation in the desert is enhanced by placing observers as high above the desert floor as possible. In rolling desert terrain, tanks and other vehicles are spread over a wide area, permitting observation in areas which cannot be seen by adjacent vehicle crews.

GSR and REMS are used to overcome visual distortion caused by the magnification by heat waves.

In a desert environment, GSRs can be used to acquire targets at extended ranges and cover considerable distances across the front.

The optimum operation of radar in desert terrain is degraded by—

- Dust and sand.
- Temperature variations.
- Static electricity.
- Wind.

To obtain the best performance in target detection, place the radar set as high as possible above the area under surveillance, so that the radar antenna overlooks the area. On smooth, sandy surfaces, the detection range for moving targets may be reduced, because sand presents a surface that does not reflect an appreciable amount of clutter. Increasing the operating angle helps to reduce this deficiency. A second disadvantage caused by the terrain is that little natural cover and concealment are available for radar positions.

It is extremely difficult to conceal combat forces and operations in flat, open terrain. Airborne collection platforms are very effective in locating concentrated enemy forces.

Foot patrols are generally limited to static defensive operations, while mobile patrols are effective in desert operations. Air reconnaissance is used to the maximum extent possible. When a unit is on a march, ground elements will normally be located at least 2,000 to 4,000 meters to the front and flank of the lead elements, depending on the terrain. OPs in static situations are sited in pairs as far apart as possible to permit accurate intersection.

The desert terrain favors wide envelopments and turning movements. The intelligence collection effort must cover all directions and use all available collection systems, especially those with long-range capabilities. Since large unit consolidations and preparations for attack are virtually impossible to hide, commanders on both sides may decide to conceal the time and place of attack through the use of deception operations. The S2 must be prepared to provide intelligence support to the S3 for deception planning. The S2 incorporates all of the collection means available in his collection plan to achieve as much redundancy as

possible. All efforts are made to confirm or deny significant indications of enemy intentions.

WINTER OPERATIONS

Because over 50 percent of the world can become a winter battlefield, the Army must be prepared to conduct IEW operations in a winter environment. This environment is characterized by low temperatures, fog, freezing rain, snow, ice, frozen conditions, and a series of freeze-thaw cycles. The effects of the winter environment on personnel and equipment are numerous. Because of the effort and extra equipment necessary to keep warm, common tasks take longer and are more difficult to perform. Mobility over frozen ground can be better than over unfrozen ground. Snow or spring mud, on the other hand, can hinder or halt movement on roads or cross country. Fog and blowing snow can reduce visibility to zero. Performance of most electro-optical systems is degraded or changed. Assessing enemy capability to live and fight in extreme cold is an essential intelligence requirement. Historically, Warsaw Pact forces conduct numerous exercises during the winter, giving them experience in conducting combat operations in cold climates. Snow and cold weather have detrimental effects on the operations of both mechanical and electronic equipment. The following factors can cause degradation of IEW operations:

- Reduced mobility of vehicle-mounted systems.
- Poor or inaccurate performance of radars, sensors, radios, and other electro-optical systems.
- Antenna icing, which can reduce range, increase noise, alter frequency, or simply collapse antennas.
- Thickened oil and lubricants, which can cause mechanical problems in generators and vehicles.
- Decrease in battery life and performance.

Certain environmental phenomena, such as snow and fog, can significantly degrade visibility, making the GSR a valuable asset. These same phenomena can affect the performance of the GSR, and must be considered by the operators. The successful operation of the radar on the winter battlefield is affected by—

- Signal scattering by ice, fog, and airborne snow.
- Variation of radar images caused by snow cover and frozen ground.
- Reduced ability of the equipment operators to function in the cold.
- Reduced battery life and performance.
- Cold- and condensation-induced maintenance problems.

Winter battlefield operations require longer periods of time to perform even simple tasks. Experience shows that five times the normal time may be needed. Therefore, increased time must be allowed in planning for set-up and relocation of the GSR.

A major impact of winter operations on equipment is caused by cold and snow. Extremely low temperatures cause metal parts of weapons to become brittle, resulting in a high breakage factor for internal parts. Vehicle engines and generators require frequent starting, and the frequent starts cause condensation in the internal parts of the engine, which later freezes. The intake filters of carburetors and C-E equipment are particularly susceptible to icing. Condensation covers on microphones and telephone handsets ice frequently if not protected. Blowing snow will also jam air-intake valves. Pneumatic antenna masts and ADP equipment freeze because of condensation. Power supplies have greatly reduced life spans. RATT equipment is very susceptible to malfunction in these circumstances. Units preparing for winter operations require a larger than normal PLL and ASL. Each unit will need larger Class III allocations because of frequent engine starting. Higher PLL usage factors will be experienced for filters, batteries, spark plugs, hydraulic hoses, and all types of seals. Thinner lubricants are required.

In winter operations, the human element is all-important and demands concerned leadership and thorough training. Particular attention must be given to minimizing the effects of vision whiteouts, with the

attendant loss of perception, which affects driving and flying. High windchill factors and the potential problems of frostbite and immersion foot are additional considerations.

Only with the proper training, planning and preparation, can IEW operations be successfully conducted on the winter battlefield.

URBAN AREAS

Urban centers have always been recognized as important strategic objectives. Commanders must not commit their forces to attack or defend an urban center unless a distinct advantage can be recognized.

Military operations on urbanized terrain (MOUT) are characterized by short engagement ranges, structured obstructions to observation and communications, extreme canalization, excellent cover and concealment, and a new vertical dimension added to the battlefield. Frequently, there are problems which include obstructions, such as rubble, control of civilian population, and reduced R&S effectiveness. These elements constrain IEW operational and sustainment capabilities.

Intelligence collection requires intensified management to be effective. The collection effort is severely hampered by the enemy's use of cover and concealment, which suppress enemy unit signatures. An urban environment, particularly one that is extensive, will eliminate many of the indicators used to determine enemy activities and disposition. The flash, sound, smoke, and dust signatures of weapons are suppressed or distorted.

Urban areas are characterized by abundant cover and concealment and limited visibility. Because of LOS considerations, the target acquisition capability of GSR within built-up areas is reduced. Inaccurate range and azimuth readings may result when the radar beam is ricocheted off buildings.

GSR will normally be used against enemy forces beyond the built-up area. Radar teams are positioned to monitor routes into and out of the built-up area. Inside the built-up area, radars are positioned to detect movement along streets, alleys, and open areas, especially during periods of limited visibility. FM 90-10 describes MOUT.

HUMINT, as with jungle and mountain operations, provides the commander with the best means of gathering intelligence.

Troop observations, reported rapidly and accurately, can contribute extensively to the collection effort. Troops supply first-hand knowledge about the location and type of enemy equipment and activity, most of which is submitted to the S3 for targeting. Interrogations of EPW, civilians, line crossers, and defectors will probably be the best source of information on enemy concentrations within the city. Civilians recently routed from their homes may provide the location of enemy forces and information on structures, such as fortifications, major facilities, and vehicle or foot bridges. HUMINT collection activity prior to the battle focuses on collection and analysis of city plans for IPB.

The urban environment restricts or limits the use of AM and FM C^2 communications. Enemy forces will make heavy use of wire and established civilian telephone systems. There will be considerable crowding on the FM band with emitters located on tall structures to afford radio LOS.

Communications and noncommunications intercepts become less valuable as an intelligence collection source. Manpack intercept and DF equipment are well suited to operations in MOUT due to their ability to be used in high-tower buildings. Vehicle-mounted ground collection systems are best used to provide early warning and indications of enemy intentions on the approaches to the urban area.

ECM also has little use in MOUT due to the perturbation of the radio LOS required for effective operations. As with the collection assets, ECM systems are best employed to provide COMJAM support in the outlying areas along suspected avenues of approach. Additionally, ECM systems are tasked with collection and early warning missions to support other ESM assets.

Because there are fewer LOS restrictions, QUICKFIX is tasked with ESM/ECM missions against the urban area. Airborne ECM systems will be useful in disrupting

the hearability of enemy C^2 links from higher echelons.

Defender advantages of cover and concealment; protected, elevated platforms for IMINT and SIGINT systems covering approaches to the urban areas; and the ability to hide key installations without risk or detection, all place a premium on good OPSEC by the approaching force. The urban environment limits the use of EW; however, airborne EW systems maybe useful in disrupting the hearability of enemy C^2 links from higher echelons.

There are no unique sustainment considerations for MI equipment, supplies or soldiers in the urban environment.

Additional information on operations on urbanized terrain is contained in FM 90-10.

MCWP 2-6

Counterintelligence

U.S. Marine Corps

5 September 2000

PCN 143 000084 00

Section 13

Counterintelligence Survey/Vulnerability Assessment Checklist

---

CLASSIFICATION

Counterintelligence Survey/Vulnerability Assessment Checklist

Background:

CI surveys/vulnerability assessments are conducted during peacetime as well as times of hostilities, both in and outside the continental U.S.

Manning of CI survey/vulnerability assessment teams should be task-organized to meet the needs/requirements of the survey; i.e., CI officers/specialists, physical security specialists from the provost marshal, communications specialists, data processing security specialists, etc.

Name of Installation
Location of Installation
Type of Installation

1. Functions, Purpose or Activities at Installation

   a. What troops, units, and command elements are stationed there or use or control the installation?

   b. What military activities (conventional, unconventional, or special) take place?

   c. What material is produced, processed, tested, or stored?

   d. What is the military importance?

2. Critical Rating of the Installation

   a. How important to national security or Marine Corps forces are the activities that take place at the installation?

   b. What activity on the installation should be veiled in secrecy? Why?

   c. What information about the installation would be of interest to hostile intelligence? Why?

   d. Is this the only location where the activities taking place can be conducted?

   e. Are there substitute places available that are suitable and practical?

Page number

CLASSIFICATION

f. Is there a key facility/organization aboard the installation?

g. Is there any sensitive or critical material or equipment stored, tested, or developed aboard the installation?

h. Is the installation a likely target for espionage?

3. Names of Principal Officers of the Installation/Organization

4. Names of Persons Directly Responsible for the Security of the Installation

5. Physical Location and Description of the Installation

a. This is the physical description of the general area surrounding the installation, paying particular attention to road networks, rail facilities, air facilities, transportation, terrain, etc.

b. Include a general physical description of the entire installation, to be accompanied wherever possible by a map, sketch or aerial photograph, and the following information:

(1) Area and perimeter.

(2) Numbers, types, and locations of buildings, and relationships among the various buildings.

(3) Roads, paths, railroad sidings, canals, rivers, etc., on the premises of the installation.

(4) Wharves, docks, loading platforms, etc., on the premises.

(5) Any other distinctive structures or features.

c. Note any particularly vulnerable or sensitive points on the installation, and the reasons for their vulnerability or sensitivity. Pay particular attention to the following:

(1) Command element/headquarters buildings.

(2) Operations/crisis action facilities.

(3) Repair shops (armor, vehicle, aircraft, weapons, and communications).

(4) Power plants.

(5) Transformer stations.

(6) Warehouses.

(7) Communications systems/facilities.

(8) Fuel storage.

(9) Water tanks, reservoirs, supply systems.

(10) Motor pools.

(11) Ammunition dumps.

(12) Aircraft.

(13) Firefighting equipment.

(14) Military police/reaction force location and reliability.

(15) Special training/testing sites.

6. Perimeter Security

a. Description of the perimeter and physical barriers.

(1) What type of fence or other physical barrier around the installation affords perimeter security?

(2) Describe the construction material of the fence/barrier.

(3) How high is the fence/barrier?

(4) Is the fence/barrier easily surmountable?

(5) Is the top protected by barbed wire outriggers?

(6) Are there any cuts, breaks, tears, holes, or gaps in the fence/barrier or any holes under it?

(7) Are there any tunnels near or under the fence/barrier?

(8) Are vehicles parked near or against the fence/barrier?

(9) Are piles of scrap, refuse or lumber kept near the fence/barrier?

(10) Is the fence/barrier patrolled and checked daily for cuts, breaks, holes, gaps, tunnels, or evidence of tampering?

(11) Where are pedestrian and vehicle gates located?

(12) Are unguarded gates firmly and securely locked?

(13) Are the gates constructed in a manner where identity and credential checks of persons or vehicles entering or exiting are accomplished, particularly during rush hours?

(14) During what hours is each gate open?

(15) Are there any railroad rights of way, sewers, tree lines, or other weak points on the perimeter?

(16) Are these weak points guarded, patrolled, or secured in any fashion?

(17) Is high intensity lighting used to light up the perimeter during hours of darkness?

(18) Where are the lights located?

(19) Are there dead spots between lighted areas?

(20) Is there backup emergency power for the lighting?

(21) Does the lighting inhibit/hamper security force observation?

7. Perimeter Security Force

a. Description of the organization of the security force.

(1) What is the strength of perimeter security forces?

(2) What are the number and location of guard posts?

(3) What is the length of perimeter covered by each post?

(4) What is the length of watch of each post?

(5) Is there a reserve backup or security force?

(6) What weapons do the guards carry?

(7) What is the level of training for each member of the security force?

(8) What instructions are given to security forces regarding identity checks/ challenges?

(9) Are there vehicle checks?

(10) Are there any watchtowers to facilitate observation of the perimeter?

(11) What are the height and location of each watchtower?

(12) Have roving patrols been utilized to patrol the perimeter? What are their number, strength, frequency, routes, and activity?

(13) What is the efficiency and manner of performance of perimeter guards and patrols?

b. Security weaknesses and recommendations.

(1) What specific weaknesses pertaining to both physical barriers and the perimeter security force were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve perimeter security?

8. Security of Buildings and Structures

a. Nature and purpose of building.

(1) Where is the location of the building?

(2) What activities take place in the building?

(3) What material/information is developed or stored?

(4) What machinery or equipment is in the building?

(5) Is the building a vulnerable point? Why?

b. Description of building—exterior, interior, and immediate surroundings.

(1) Describe the design and construction of the building.

(2) How many stories? Height?

(3) Does the building have a basement?

(4) What percentage is wood?

(5) What percentage is concrete?

(6) What other materials are used in the exterior?

(7) Describe walls.

(8) Describe floors.

(9) Describe ceilings.

(10) Describe roof.

(11) Is the building safely designed and constructed?

(12) Is the building properly maintained and constructed?

(13) Check locations of doors, windows, sewers, sidewalks, elevators, stairs, fire escapes, skylights, crawl spaces/false ceilings, and any other possible means of exit or entry.

(14) Are these entrances properly locked, or otherwise safeguarded against unauthorized entry?

(15) Are windows and skylights screened, grilled, or barred?

(16) Can unauthorized or surreptitious entry be effected in any manner?

(17) Are exit and entry facilities adequate to meet an emergency situation?

(18) Are all keys to building controlled?

(19) Where is the key control maintained?

(20) Who maintains the key control?

(21) How rigorously is it kept?

(22) Who is authorized to receipt for the keys?

(23) Are any measures taken to restrict entry into the building; i.e., pass, badges, access rosters, etc.

(24) Are controlled access methods enforced?

(25) If the building is determined to be sensitive, high threat priority, or vulnerable, has it been declared as restricted, and is the area surrounding it so designated?

(26) Are daily security checks conducted at the end of each working day in areas where classified material is stored? Are all security containers checked?

c. Guard and patrol system around the building.

(1) What are the duties of guards and patrols?

(2) Are high intensity lights used to light up the exterior and the area surrounding the buildings during hours of darkness?

(3) Is there a reactionary security force?

(4) What is the response time? Has it been tested?

(5) What is the size of the guard force? Reactionary force?

(6) What are the means of activating the reactionary force? Are there backup systems?

d. Security of electrical equipment.

(1) Is there auxiliary lighting?

(2) Are circuit breakers properly protected?

(3) Are telephone junction boards protected?

e. List the frequency of periodic checks made throughout the building to detect the following:

(1) Holes, cracks, crevices that might conceal explosives, incendiary devices, or audio/visual monitoring devices. Are such repaired?

(2) Tampered wiring, or broken or electrical connections and wires.

(3) The presence of suspicious packages or bundles.

(4) Any dangerous practices, including safety, electrical, or fire hazards that may result from negligence or deliberate attempts at sabotage,

f. Security weaknesses and recommendations.

(1) What specific weaknesses pertaining to the security of interiors and exteriors were noted during the survey?

(2) What specific reasonable recommendations may be made to improve the security of the buildings?

9. Security of Docks, Wharves, and Platforms

a. Description of the location, nature, and purpose of each dock, wharf, or platform.

(1) What administrative supervision of the docks, wharves, and loading platforms is exercised? By whom?

(2) What type of security force provides protection for each?

(3) What measures are taken to prevent loitering in the vicinity of each?

(4) What measures are taken to prevent unauthorized observation of loading and unloading?

(5) What protection is afforded mechanical sabotage, arson, explosion, or dangerous practices?

(6) Are same precautionary measures taken as outlined for access to building interiors and exteriors?

b. Traffic conditions.

(1) Are inspections of deliveries made to guard against sabotage devices; i.e., explosives, caustic chemicals, etc.?

(2) What precautions are taken to conceal the loading and unloading of personnel or material if such handling requires secrecy?

(3) Are delivery trucks, railroad cars, and privately owned vehicles checked for possible sabotage devices?

(4) How much is the movement of drivers and helpers aboard the installation controlled?

(5) In the case of movement of personnel, equipment, and material, are identifying markings removed in an effort to assist in operations security?

c. Security weaknesses and recommendations.

(1) What specific weaknesses pertaining to the security of docks, wharves, and loading platforms were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of docks, wharves, and loading platforms?

10. Motor Pools, Dismount Points, and Parking Areas

a. Security measures at each facility.

(1) Are motor pools, dismount points, and parking areas adequately guarded?

(2) Are vehicles properly checked and accessible only to authorized personnel?

(3) What system of checking vehicles is used?

(4) What measures are taken to safeguard fuels, lubricants, tools, and equipment against sabotage, theft, fire, and explosion?

(5) Are frequent checks made of all vehicles for possible mechanical sabotage?

(6) Are drivers and mechanics instructed as to the proper checks to be made to guard against or detect sabotage?

(7) What provisions are made to prohibit privately owned vehicle parking in motor pools, dismount points/parking areas?

(8) Are fuels and lubricants frequently tested for possible contamination?

(9) Are parking/staging areas restricted or supervised in any way?

(10) Are parking arrangements consistent with security against sabotage, terrorist, or other hazards?

(11) What provisions are made for visitors parking?

(12) Do parking arrangements/facilities impede efficient traffic flow through and near the compound?

(13) Would parking arrangements interfere with firefighting or other necessary emergency vehicles if there were an emergency?

b. Security weaknesses and recommendations.

(1) What specific weaknesses about the security of motor pools and parking lots were noted during this survey?

(2) What specific and reasonable recommendations may be made to improve the security of the motor pool and parking lots.

11. Power Facilities and Supply

a. Description of supply, facilities, and security measures.

(1) What type of power is used by the installation?

(2) What is the peak load of electric power?

(3) What percentage of the electric power is generated on the installation?

(4) What is the installation's electric generating capacity?

(5) What percentage of electric power is purchased from outside sources?

(6) Are all current sources ample to provide a reserve beyond full load demands?

(7) From whom is the electric power purchased?

(8) Is an alternate or auxiliary electric power system available for emergency use?

(9) Can the auxiliary electric power system be used immediately?

(10) How many and what kind of power substations/transformers are on the installation?

(11) Are control panels, pressure valves, gas facilities, and control valves in good working order? How frequently are they checked? Is adequate fire protective equipment available and nearby?

(12) Are power substations/transformers adequately safeguarded against trespassers and saboteurs?

(13) Are generators properly maintained and checked with particular emphasis on oil levels and temperatures?

(14) Are combustible materials removed from their vicinity?

b. Miscellaneous features:

(1) Are replacement units for generators and motors available in safe storage?

(2) Do transformers have sufficient capacity? Are they safely located and well-protected by physical barriers and guards?

(3) Are oil-filled transformers located in noncombustible well-drained buildings or outside?

(4) Are frequent inspections made of the oil, contact, and control apparatus of circuit breakers and transformers?

(5) What is the system of power lines in use?

(6) What is the number of independent power feeds?

(7) Is the pole line or underground line safe, reliable, and frequently checked?

(8) Are all power lines protected by lightning arresters?

(9) Are power distribution lines properly installed and supported?

(10) Are electric circuits overloaded at any time?

(11) Are current national or civil electric codes followed?

(12) Is there a single or multiple main switch(s) for emergencies?

c. Security weaknesses and recommendations.

(1) What specific weakness about the security of power facilities and supply were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of power facilities and supply?

12. Fire Fighting Equipment and Facilities

a. Describe the amount and condition of equipment and facilities.

(1) What fire fighting and first aid equipment are available on the installation?

(2) What types of fire extinguishers are available; i.e., foam, dry chemical, halon, water, carbon dioxide, and carbon tetrachloride? Are they at locations where such types may be needed?

(3) Are all extinguishers and other equipment in working order and frequently tested and inspected?

(4) Are fire extinguishers sealed to prevent tampering?

(5) Do competent personnel make inspections of fire equipment and record results recorded?

(6) Are both first aid and firefighting equipment painted to be conspicuous? Are they within reach of all personnel, unobstructed, and of reasonable size and weight to permit ease of handling by all personnel?

(7) Is first aid equipment available? Does it include ample amounts of materials needed?

(8) Are first aid supplies checked periodically and safeguarded?

(9) What type of fire alarm system(s) is/are installed?

(10) Are there sufficient numbers of alarms and sensors in the system?

(11) Is the fire alarm system frequently inspected and tested?

(12) Are vulnerable and/or important facilities equipped with sprinkler systems?

(13) What type of sprinkler system(s) is/are used? Are they fed by public mains, tanks, private reservoir, or pumps?

(14) How often and thoroughly is the sprinkler system inspected?

(15) Where are the main control valves of the system located?

(16) Are fire hydrants near vulnerable or important facilities?

(17) Are hydrants in working order? How often are they inspected and tested?

(18) Is the water pressure sufficient so that streams of water will reach and extinguish flames in all sections of the installation?

(19) Is there a secondary source of water supply available?

(20) Does the installation have its own fire department? A brigade? What equipment does it have? Are the personnel well trained?

(21) Have arrangements been made with public fire departments to furnish equipment and personnel to augment the installation department/brigade?

(22) Is the nearest public fire department paid or is it a volunteer unit?

(23) Has a program of fire drills been inaugurated? Are such drills conducted in an efficient and earnest manner?

(24) Has a fire prevention program been inaugurated?

(25) What plans have been made for the action of all personnel if there is a fire?

b. Security weaknesses and recommendations.

(1) What specific security weaknesses about the firefighting equipment and facilities were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of firefighting equipment and facilities?

13. Water Supply

a. Description of water supply and security measures taken to safeguard it.

(1) What sources of water supply are used by the installation?

(2) Are sources of water reasonably safe, adequately guarded, and protected by physical security?

(3) If a public supply is used, what is the diameter of the main line?

(4) What is the water pressure? Is it adequate for normal use as well as for emergencies?

(5) If a private reservoir or tank is used, what is its capacity, level, pressure, and condition?

(6) Is it adequate for the installation's needs?

(7) What type of pumps are used in the water system (underwater, suction, centrifugal, electric, etc.)?

(8) Are water pumping stations adequately protected, frequently inspected, and tested?

(9) Are all valves secured properly?

(10) Is a supplementary water system available? Where? Is it secure?

(11) How often is water tested for purification? By whom? Is the water treated? By whom? By what chemicals?

(12) Are taps/sources of unpotable water adequately marked?

(13) Is the sewage system adequate for the installation?

(14) Are sewer mains, control, pumps, and disposal systems adequate?

(15) Is there a possibility of water or food contamination from the sewage system?

(16) Has there been any epidemic outbreak at the installation traceable to waste disposal?

b. Security weaknesses and recommendations.

(1) What specific and reasonable recommendations may be made to improve the security of the water supply?

(2) What specific weaknesses about the water supply were noted during the survey?

14. Food Supply

a. Description of security measures.

(1) From what sources does the installation receive food and allied supplies? Can these sources be considered reliable?

(2) If food supplies are purchased from merchants and farmers in the local vicinity, have they been checked and tested for cleanliness?

(3) Have caterers and companies or individuals who operate food, candy, soft drink, or other concessions on or near the installation been checked? Have their products been thoroughly tested?

(4) Have local food handlers been checked for health, cleanliness, and loyalty?

(5) Is entry to kitchens and food storerooms restricted to authorized personnel? How are such restrictions enforced?

(6) Are pantries and refrigerators locked when not in use?

(7) Are kitchens and storerooms in sanitary condition?

(8) Is there any evidence of unsanitary conditions?

(9) Are frequent checks made of foods, drinks, etc., to prevent or detect toxicological or bacteriological sabotage?

(10) Has there been any epidemic or excess absenteeism traceable to food or water supplies of the installation?

b. Security weaknesses and recommendations.

(1) What specific weaknesses about the security of the food supply were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of the food supply?

15. Communications Facilities

a. General service and special communications message centers.

(1) Description.

(2) Where is the message center located?

(3) Is the message center adequately protected by physical barriers and guards?

(4) Is someone on duty at the message center at all times?

(5) Who handles the mail at the message center? Have mail handlers been subject to background and local records checks?

(6) Are all encryption (hardware and software) devices properly safeguarded and properly destroyed when obsolete?

(7) Are logs kept of authorized couriers and message traffic distribution?

(8) Are unauthorized personnel excluded from the message center?

(9) Are classified messages handled in accordance with OPNAVINST 5510.1

(10) Through what channels do classified messages pass?

(11) Have messengers, couriers, and operators been checked? Do they have appropriate security access(es)?

b. Security weaknesses and recommendations.

(1) What specific weaknesses about the security of the communications systems were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of the communications system?

16. Wire and Wireless Communications Equipment

a. Description.

(1) What means of wire and wireless communications are used throughout the installation?

(2) Where are the central points of such communications networks located?

(3) Are switchboards adequately guarded?

(4) Have operators been checked and cleared?

(5) Is auxiliary power available?

(6) Is auxiliary or replacement equipment available?

(7) Are open wires, terminal boxes, cross-connecting boxes, cables, and manholes frequently inspected for indications of sabotage and/or wire-tapping?

(8) Are maintenance crews alerted to search for tapping?

(9) Are civilian repairmen used? Are they checked and cleared?

(10) Have preparations been made to take care of sudden breaks in the system efficiently?

(11) Have personnel been cautioned about discussing classified or sensitive matters over unsecured telephone, teletype or radios?

b. Security weaknesses and recommendations.

(1) What specific weaknesses about the security of the communications system were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of the communications system?

17. Security of Information

a. Where on the installation are plans, blueprints, photos, classified material/ equipment, or other information of value to the enemy kept? The following list is not all-inclusive and is not a replacement for the checklist in OPNAVINST 5510.1.

(1) Is such material centralized in a single facility or scattered through various offices or buildings?

(2) In what sections is classified material processed stored and what level of classification is authorized in each area?

(3) Is all classified or valuable information kept in authorized/approved security containers or vaults?

(4) Are fight safes and cabinets affixed to floors or chained to immovable objects?

(5) Are container doors closed and locked when not in use?

(6) Is there any protection other than the container itself.

(7) What protection is given to a combination of containers?

(8) What security measures are enforced about keys to doors, gates, or file cabinets?

(9) Is access limited to combinations and keys?

(10) Who has access to combinations and keys? Do all authorized personnel have access? Have they been cautioned about passing keys and combinations to unauthorized personnel?

(11) Is a rigid chain of custody required for classified information (Secret and above)? Can custodians identify the location of classified at any time?

(12) Are only personnel with completed background checks and appropriate access assigned to positions requiring the handling of classified material?

(13) Are plans, blueprints, reports, or other classified material returned promptly and properly turned in?

(14) Who has access to classified material (with and without approved access)?

(15) Is dissemination of classified material strictly limited to those with a need to know?

(16) Is rank or position considered sufficient reason for access to classified information?

(17) Is classified material left unattended on desks where persons passing by can observe or steal without detection?

(18) Have civilian janitors been checked and placed under supervision?

(19) How is classified waste disposed of? Are destruction records kept?

(20) What policy has been established regarding releases and statements to local or national news media?

(21) Have all personnel been cautioned about unauthorized statements and releases?

b. Security of personnel.

(1) What specific weaknesses about the security of information were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of information?

18. Security of Personnel

a. OPNAVINST 5510.1 provides guidelines on personnel security.

b. Who is responsible for the security of the installation?

c. What is their attitude towards security?

d. Is the command aware of continuous evaluation of those who have access to classified or sensitive material or equipment?

e. Are personnel in positions of trust and confidence considered reliable?

f. What is their attitude towards security?

19. Identification System

a. What system is used to identify personnel authorized access within the confines of the installation/facility?

b. If badges are used—

(1) Are badges or identification cards of tamper-proof design and difficult to reproduce or counterfeit?

(2) Is the makeup and issue of badges and identification cards rigidly controlled to prevent:

(a) Reproduction?

(b) Theft?

(c) Unauthorized use or issue?

(d) Failure to return to issuing authority?

(3) Are photographs used on the face of the cards/badges?

(4) Is a detailed description used to positively identify holder?

(5) Are color or coded systems used to identify level of access for department personnel granted access?

(6) Are specific badges valid for specific areas?

(7) Is enforcement of such identification rigid?

(8) Do regulations prescribe that everyone wears the badge at all times and are regulations enforced?

(9) Is admittance to the installation/facility governed by the identification system?

(10) When badges are reported missing, lost, or forgotten what action is taken?

c. Is entrance permitted by wearing a military uniform?

(1) What other MEANS of identification are used?

(2) Are access rosters passed from one facility/command to another via secure means?

(3) Are passes or identification cards closely scrutinized?

d. What system is used to prevent persons working in one building, section, or unit from wandering about restricted areas without proper authorization?

20. Visitor Controls

a. What system is used to identify and admit authorized and legitimate visitors to the installation or facility?

(1) How and by whom is the legitimacy or necessity of a visitor's mission established?

(2) Are regulations lax in the control of visitors?

(3) On arrival at the gate, entrance of the facility or section, are visitors escorted to a reception area?

(4) Are regulations lax in the control of visitors?

(5) Is the identity of visitors verified?

(6) Is adequate information obtained from visitors?

(7) Is the purpose of the visit obtained?

(8) Are visitors required to register in a logbook with the following information?

(a) Full name.

(b) Social security number.

(c) Rank.

(d) Parent Organization.

(e) Date and time of entry.

(f) Time of departure.

(g) Number of security badge issued and level of access.

(h) Reason for visit.

(i) Name of official authorizing entry or providing escort.

(9) Are visitors required to provide identity on departure?

(10) Are visitors escorted or kept under surveillance during the time they are on the installation?

b. Is a vehicle register kept which includes:

(1) Date and time of entrance.

(2) Registration numbers.

(3) Name of owner(s).

(4) Signatures of driver(s) and passengers.

(5) Brief description of contents of vehicle.

(6) Inspections conducted on vehicle.

(7) Time of departure.

c. Are news media carefully checked and verified?

(1) Are credentials examined and verified?

(2) Has their visit been checked with higher commands to verify authority?

d. Are orders and credentials of allied military personnel examined by competent personnel (linguists, etc.).

(1) Are such visits verified by higher authority?

(2) Is security unduly sacrificed to courtesy?

e. Are spot checks of persons within the installation/facility made from time to time?

f. Security weaknesses and recommendations.

(1) What specific weaknesses about identification and visitor control were noted during the survey?

(2) What specific reasonable recommendations may be made to improve security by further identification and visitor control?

21. Description of Guard System

a. General description of the guard force.

(1) Strength.

(2) Shifts.

(3) Reserves.

(4) Weapons.

(5) Training.

(6) Number and type of posts.

(7) Communications.

b. Check the following points.

(1) What is the organization of the guard force?

(2) What is the numerical strength of each shift or relief?

(3) How many shifts or reliefs are there?

(4) How many supervisors does each shift have?

(5) Is supervision of the guard force adequate?

(6) How many fixed posts does the force cover?

(7) Where is each post located?

(8) How many patrols are covered by the guard force?

(9) What is the route of each patrol?

(10) Are routes of the patrols varied?

(11) What is the time of each patrol?

(12) Are doors and gates closely checked by the patrols?

(13) What functions are performed by the patrols?

(14) Does the supervisor make inspection tours of the routes?

(15) How frequently and thoroughly are such tours made?

(16) Are inspections varied as to route and time?

(17) Are guard force communications and alarm systems in use? Are they adequate?

(18) What type of communication and alarm system does the guard force have? Are there backup systems?

(19) Is a record kept of all guard force activity?

(20) Does the guard force have communications with the military police?

(21) What armament does the guard force have?

(22) Are the weapons in serviceable condition?

(23) Are the weapons suitable for the mission?

(24) Are arms and ammunition adequately safeguarded when not in use?

(25) Is there a record of custody when weapons are issued during each shift?

(26) Where are the weapons and ammunition stored? Does storage prevent rapid access to the guard force?

(27) How are guards recruited?

(28) What physical, mental, age, or other qualifications must protective guards have?

(29) How thoroughly are prospective guards investigated?

(30) Are guards uniformed, and do they have credentials or badges? What other system of identification is used?

(31) Is the guard force competent and respected by personnel of the installation?

(32) How thoroughly is the guard force trained?

(33) How much time is spent on training the guard force?

(34) How is the training of the guard force conducted?

(35) Does such training cover the following points?

(a) Care and use of weapons and ammunition.

(b) Common forms of espionage and sabotage activity.

(c) Common forms of bombs explosives.

(d) Familiarization with the installation/facility, with particular emphasis on restricted and vulnerable areas.

(e) Location and character of hazardous material and processes.

(f) Location and operation of important steam and gas valves and main electrical switches.

(g) Location and operation of fire protective equipment including use of sprinkler control valves.

(h) Conditions that may cause fires and explosions.

(i) Location and use of all first aid equipment.

(j) Duties in the event of fire, blackouts, or other emergencies that can be foreseen.

(k) Use of communication systems.

(l) Observation and description.

(m) Preservation of evidence.

(n) Patrol work.

(o) Searches of persons and places.

(p) Supervision of visitors.

(q) General and special guard orders.

(r) Location of all guard posts.

(36) Do guards have keys to gates, buildings, and offices?

(37) Do guards check the credentials of visitors and personnel working on the installation or facility?

(38) Is the strength of the guard force consistent with -

(a) Number of pedestrian, vehicle, and railroad gates and the hours they are open?

(b) Approximate number of daily visitors? Proper visitor reception?

(c) Number of loading platforms, storage facilities, working areas, etc.?

(d) Number of vehicles to cover the entire installation in a reasonable time?

(e) Number of restricted areas and vulnerable points?

(f) Number of plants or pumping stations?

(g) The number and extent of parking areas?

(h) Necessary supervision of the guard force?

(i) Sickness, leave, injury, etc., of guard personnel?

(39) What are the duties of the guard force if there are security violations? Does the guard force have security clearance and access?

c. Guard headquarters.

(1) Is the guard headquarters conveniently located?

(2) Is the guard headquarters properly secured at all times, and does it contain necessary equipment?

(3) Does the guard headquarters contain adequate facilities for members of the guard force?

d. Security weaknesses and recommendations.

(1) What specific security weaknesses were noted during the survey of the installation’s guard force?

(2) What specific and reasonable recommendations regarding the guard force may be made to improve the security of the installation?

22. Description of Security Conditions and Security Measures of Adjacent Areas

a. What is the general nature of the population and the area surrounding the installation?

(1) Does the nationality or political nature of the surrounding populace offer a natural cover and aid to hostile agents and saboteurs?

(2) Is the installation within a commercial air zone of travel?

(3) If so, are minimum altitudes for planes published at all local airports?

(4) Is the installation isolated or screened from public view?

(5) Are restricted areas screened or isolated from public curiosity?

(6) Is the installation exposed to hazards brought onto the installation by natural conditions such as floods, extreme winds, forest fires, electrical storms, etc.?

(7) Is the installation or buildings within the installation well camouflaged against both air and ground observation?

(8) Have places of amusement near the installation and persons frequenting them been investigated, scrutinized, and checked?

(9) Have nightclubs, poolrooms, bowling alleys, houses of prostitution, barbershops, restaurants, taverns, stores, and other places frequented by personnel from the installation been included and thoroughly checked.

(10) Has the surrounding area been carefully scrutinized for any place likely to be used as bases for espionage or sabotage agents? Areas that could conceal antennas, audio and visual surveillance, etc.?

b. Security weaknesses and recommendations.

(1) What specific security weaknesses were noted during the survey of the area adjacent to the installation?

(2) What specific and reasonable recommendations may be made to improve security?

23. Security of Air Installations. The security of air installations does not differ from any other installation. Aircraft and maintenance facilities are high priority targets of saboteurs and espionage agents. In general, checking the following major areas will assist in establishing the security afforded to the installation.

a. Is the guard system adequate?

b. Are individual aircraft guarded sufficiently?

c. Are hangers and other vital buildings in a restricted area?

d. Have precautions been taken to see that there is no smoking in the area?

e. Are aircraft stored in hangers inspected periodically against sabotage?

f. Are special precautions taken to ensure visitor control in hangars?

g. Are vital repair parts in storage areas protected from unauthorized personnel, fire, and the elements?

h. Are there fire trucks, crash and rescue vehicles available?

i. Is emergency equipment parked in a convenient location readily available to any part of the installation?

24. Practical Use of Security Checklist

a. This checklist is not all encompassing and should be used as a guide to initiate a survey. Several methods of organizing a security check may be used. The following methods have been found to be practical and efficient.

(1) Itemize on index cards or automated data file requirements listed on the checklist and write the required information on each card/file as it is checked off the list.

(2) Itemize basic subdivisions of survey checklist requirements on separate pages with itemized requirements listed in required order. Write in the required information in the proper space as each item is checked off.

(3) Itemize all requirements of the survey checklist on separate pages, subdividing the pages according to main subdivision requirements. Make detailed notes about each item as it is checked off.

b. After completing notes on all requirements for each item, assemble in order and prepare report.

FIELD MANUAL 34-130

*FM 34-130
Headquarters
Department of the Army
Washington, DC, 8 July 1994

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

Table of Contents

Page

PREFACE iv

CHAPTER 1—INTRODUCTION 1-1
What is IPB? 1-1
Step 1. Define the Battlefield Environment 1-1
Step 2. Describe the Battlefield's Effects 1-2
Step 3. Evaluate the Threat 1-2
Step 4. Determine Threat COAs 1-3
Who Conducts IPB? 1-3
Doctrine Versus Tactics, Techniques, and Procedures 1-4
What IPB Accomplishes 1-5
IPB and the Intelligence Estimate 1-5
IPB and the Decision Making Process 1-6
IPB and the Targeting Process 1-9
IPB and the Collection Management Process 1-9
IPB and the Command and Staff Execution of Battle 1-12
How IPB Relates to Everything Else 1-13

CHAPTER 2—CONDUCTING INTELLIGENCE PREPARATION OF THE BATTLEFIELD 2-1
How to Conduct IPB 2-1
Define the Battlefield Environment 2-2
Describe the Battlefield's Effects 2-7
Evaluate the Threat 2-29
Determine Threat Courses of Action 2-39
The Abbreviated IPB Process 2-52

CHAPTER 3—EXAMPLE APPLICATIONS OF INTELLIGENCE PREPARATION OF THE BATTLEFIELD 3-1
Scenario One: Conventional Offense 3-1
Scenario Two: Conventional Defense 3-43

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

* This publication supersedes FM 34-130, 23 May 1989.

Weather Analysis
USAF weather teams at division, corps, and EAC work together with engineer teams during much of the analysis process. The weather team analyzes the weather's direct effects and its effects on terrain and integrates climatic, forecast, and current weather data with terrain analysis.

Terrain and weather analyses are inseparable. You should have already included the weather's effects on terrain during terrain analysis. In this sub-step, weather analysis evaluates the weather's direct effects on operations.

If time and resources permit, you can obtain climatology-based overlays for planning purposes from the USAF Environmental Technical Applications Center. Once deployed, the supporting USAF weather team can prepare similar but less detailed overlays depending on the availability of data. Weather teams can provide detailed descriptions of the weather's effects on each system and sub-system of your unit's equipment. If you are not directly supported by a weather team, request support from your higher headquarters.

Evaluate the effects of each military aspect of weather. However, just as in terrain analysis, focus on the aspects that have the most bearing on the situation your command faces. Begin the evaluation of each aspect with the local climatology, but always free-tune the evaluation with the most current forecast available.

You use two sub-steps to accomplish weather analysis: (1) Analyze the military aspects of weather; and (2) Evaluate the weather's effects on military operations.

Each sub-step is discussed below.

(1) ANALYZE THE MILITARY ASPECTS OF WEATHER.

The military aspects of weather are—

Visibility:
Low visibility is beneficial to offensive and retrograde operations. In the offense, it conceals the concentration of maneuver forces, thus enhancing the possibility of achieving surprise. Low visibility hinders the defense because cohesion and control become difficult to maintain, R&S are impeded, and target acquisition is less accurate.

When evaluating visibility, consider the effects of all aspects of the weather. For example, temperature conditions can have either an adverse or beneficial effect on the use of modern thermal sights. Cloud cover can negate the illumination provided by the moon. Precipitation and other obscurants can also have varying effects.

A major factor in evaluating visibility is the amount of available light. Consider the phase of the moon as well as the times associated with—

- Beginning morning nautical twilight (BMNT).
- Sunrise.
- Sunset.
- End evening nautical twilight (EENT).
- Moonrise.
- Moonset.

Winds:
Winds of sufficient speed can reduce the combat effectiveness of a force downwind as the result of blowing dust, smoke, sand, or precipitation. The upwind force usually has better visibility. NBC operations usually favor the upwind force.

Strong winds and wind turbulence limit airborne, air assault, and aviation operations. Evaluation of weather in support of these operations requires information on the wind at the surface as well as at varying altitudes. High winds near the ground increase turbulence and may inhibit maneuver. High winds at greater altitudes can increase or reduce fuel consumption.

Wind-generated blowing sand, dust, rain, or snow can reduce the effectiveness of radars and communication systems. Strong winds can also hamper the efficiency of directional antenna systems by inducing antenna wobble.

Precipitation:
Precipitation affects soil trafficability, visibility, and the functioning of many electro-optical systems. Heavy precipitation can reduce the quality of supplies in storage. Heavy snow cover can reduce the efficiency of many communication systems as well as degrade the effects of many munitions and air operations.

Cloud Cover:
Cloud cover affects ground operations by limiting illumination and the solar heating of targets. Heavy cloud cover can degrade many target acquisition systems, the use of infrared-guided artillery, and general aviation operations.

Heavy cloud cover often canalizes aircraft within air AAs and during the final approach to the target. Partial cloud cover can cause glare, a condition that attacking aircraft might use to conceal their approach to the target. Some types of clouds reduce the effectiveness of radars.

Temperature and Humidity:
Extremes of temperature and humidity reduce personnel and equipment capabilities, and may require the use of special personnel shelters or equipment. Air density decreases as temperature and humidity increase, which may require reduced aircraft payloads.

Temperature "crossovers," when target and background temperatures are nearly equal, degrade the use of thermal target acquisition systems. The length of crossover time depends on air temperature, soil and vegetation types, amount of cloud cover, and other factors.

(2) EVALUATE THE WEATHER'S EFFECTS ON MILITARY OPERATIONS.

Weather has both direct and indirect effects on military operations. Examples of indirect effects are—

- Temperature inversions might cause some battle positions to be more at risk to the effects of chemical warfare than others due to their altitude.
- Local conditions of visibility, such as fog, might make some potential engagement areas more attractive than others.
- Hot, dry weather might force a unit to consider water sources as key terrain.

All of these conditions would significantly affect the selection of defensive positions even though their effects are indirect. An effective technique for evaluating and depicting the

weather's indirect effects is to modify the terrain analysis products to show the effects of weather considerations.

Remember to revise the effects of weather upon terrain analysis as the weather changes from the originally evaluated conditions.

You must also evaluate the weather's direct effects on personnel, equipment, and operations. Begin by establishing the critical values of the military aspects of weather that affect the effectiveness of—

- Personnel.
- Specific types of equipment.
- Types of military operations.

An example would be setting critical values for visibility's effects on airborne operations as—

- Visibility of 1 km or less as an unfavorable condition.
- Visibility of 1 to 5 km as a marginal condition.

A forecast of 2 km visibility can then be quickly evaluated as making the conditions for airborne operations marginal.

See Appendix B for other examples and techniques in establishing critical values. An example of critical values arranged into matrix format is shown at Figure 3-1-13.

Once you have set the critical values, use them as gauges to evaluate the effects of local weather on the operations and COAs available to both friendly and threat forces.

An example might be an S2 reporting to his commander: "Sir, weather practically rules out the use of air assault operations because temperature and humidity have reduced the lift capability of the enemy's helicopters by 70 percent."

Weather effects are harder to depict graphically and may have to be portrayed in a matrix.

Figure 2-9 is an example of one type of matrix that shows the results of the evaluation of the weather's effects on military operations. See Chapter 3 for other examples.

Regardless of the means of presentation, ensure you focus on the *effects* of weather on military operations rather than the factors that make up the analysis.

For example, you might express the effects of visibility and precipitation on the mobility of a force in terms of movement rates or the amount of time the force will be exposed in an engagement area. These types of evaluations are more readily usable by the commander than statements such as "...3 inches of rain over the next 24 to 48 hours..."

Additional Considerations:

- To completely account for the weather's effects on your unit's equipment, you must account for its effects on each system and subsystem. For example, when considering the weather's effects on a tank, you must consider its effects on—
  - Target acquisition systems.
  - Ballistic trajectories.
  - Mobility.
  - Crew performance.

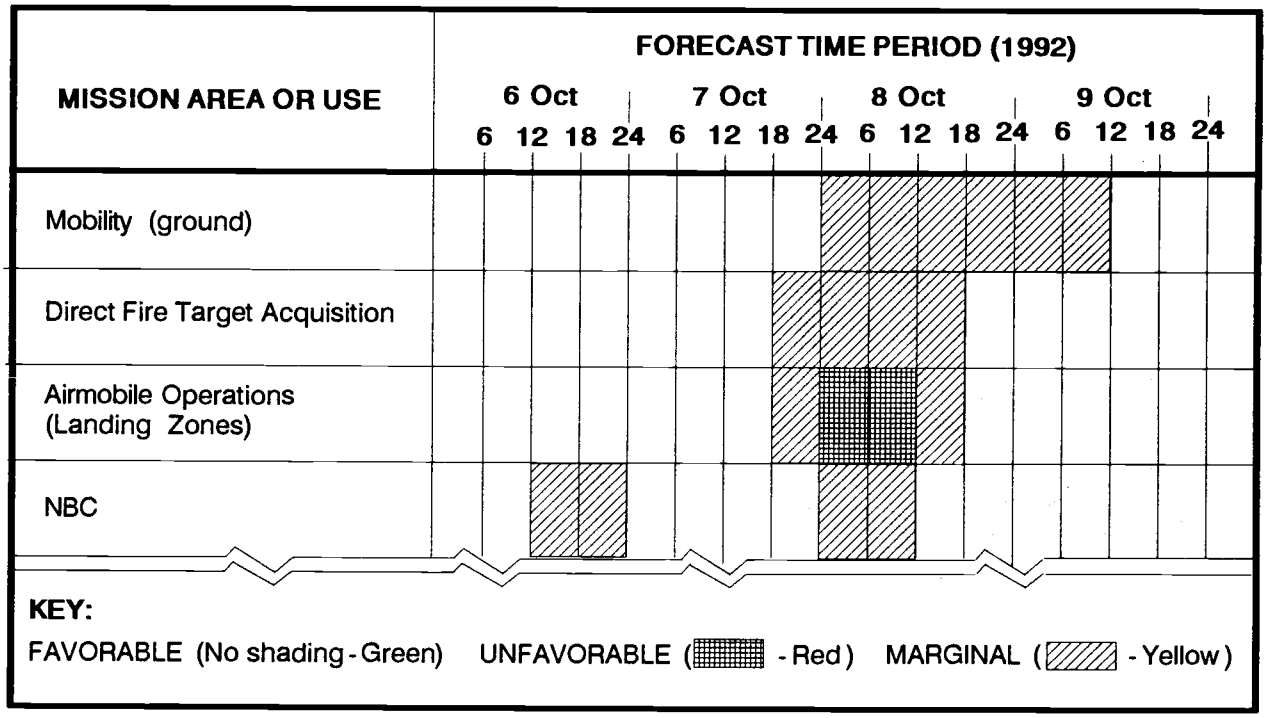


Figure 2-9. Determine the weather's effects on military operations.

- You do not have the equipment or information needed to conduct detailed weather analysis. **Use the supporting weather team!**

For more information, refer to—

- FM 34-81-1 for "how to" information on determining the weather's effects on military operations.
- FM 34-81/AFM 105-4 for information on support by USAF weather teams.

Analysis of Other Characteristics of the Battlefield

"Other Characteristics" include all aspects of the battlefield environment that affect friendly or threat COAs not already incorporated into the terrain and weather analysis.

An example might be an S2 reporting to his commander: "Sir, religious considerations will make cordon and search operations on Wednesdays extremely difficult to execute—the local population will be praying at the same time we're trying to conduct the search."

In another example, during riot control assistance to civil authorities the influence of gangs or other unofficial political elements becomes very important.

Use a two step process to determine the effects of other characteristics of the battlefield:

(1) ANALYZE THE OTHER CHARACTERISTICS OF THE BATTLEFIELD.

Typical Characteristics: Because these aspects vary greatly with each circumstance, a comprehensive list cannot be provided here. However, depending on the situation, these characteristics might include:

- Logistics infrastructure, such as—

- Land use patterns.
- Sources of potable water.
- Bulk fuel storage and transport systems.
- Canals and waterways, with associated control facilities such as locks.
- Communication systems.
- Transportation means and systems, including road and rail networks, transloading facilities, and airfields.
- Natural resources.
- Industries and technologies.
- Power production facilities.
- Chemical and nuclear facilities.

- Population demographics, such as—
  - Living conditions.
  - Cultural distinctions.
  - Religious beliefs.
  - Political grievances.
  - Political affiliation.
  - Education levels.
- Economics.
- Politics—local, regional, and international (government systems, treaties, agreements, and legal restrictions; includes unofficial systems such as gangs).

(2) EVALUATE THE EFFECTS OF OTHER CHARACTERISTICS OF THE BATTLEFIELD ON MILITARY OPERATIONS.

As with terrain and weather, the evaluation of the other characteristics of the battlefield is not complete until you express it in terms of their effects on friendly and threat COAs.

In some situations, the "other characteristics" of the battlefield are of more concern than terrain and weather. An historical example illustrates this well:

> All US Army activities during and preceding Operation JUST CAUSE were bound by the Carter-Torrijos treaty. Certain provisions of this treaty categorized land within the old canal zone into five different categories. The rights and responsibilities of the United States and the Republic of Panama varied widely depending upon the legal designation of the terrain.
>
> During the show of force operations that led to JUST CAUSE, the legal status of each piece of land influenced the COAs of US Forces and Panamanian Defense Forces far more than the tactical significance of the terrain and weather.
>
> To further illustrate this point, the perception of "seizing the moral highground" often influenced the actions of both sides in Panma far more than the terrain and weather.

These other characteristics of the battlefield are particularly important at the operational and strategic levels, but also play a major role at the tactical level in operations other than war. Chapter 5 gives examples of "other characteristics" as they might affect operations at different levels of war.

Although you will usually be forced to discuss the effects of other characteristics of the battlefield in text products or a matrix, always attempt to use graphics. Examples of graphic depictions include an overlay showing areas most vulnerable to insurgent operations, based on demographics; or an overlay identifying HVTs in the logistics infrastructure, in either the threat or friendly rear area.

DESCRIBE THE BATTLEFIELD'S EFFECTS ON THREAT AND FRIENDLY CAPABILITIES AND BROAD COURSES OF ACTION

Combine the evaluation of the effects of terrain, weather, and the other characteristics of the battlefield into one integrated product. Do not focus on the factors that lead to your conclusions. Instead, focus on the total environment's effects on COAs available to both friendly and threat forces.

The following are some examples of techniques for accomplishing this.

- Prior to the development of friendly COAs—
  - Provide the evaluated and prioritized set of AAs to the S3 so he can develop COAs by designating an axis of advance, direction of attack, or zone of attack for each subordinate unit (offense).
  - Provide the sets of defensible terrain along threat AAs to the S3 so he can develop strongpoints, battle positions, or sectors for each subordinate unit (defense and retrograde).
  - Identify the periods when weather conditions will optimize the use of friendly sighting and target acquisition systems so the S3 can make recommendations on the timing of operations.
- After the development of friendly COAs, emphasize concluding sentences, such as "... of the COAs available, COA 2 makes second best use of the opportunities the battlefield environment offers for the following reasons..."

You must address the battlefield's effects on threat as well as friendly COAs. A good technique for accomplishing this is to completely place yourself in the perspective of the threat's S2 and S3 who must recommend a set of COAs to their commander.

Ensure that you evaluate the effects of battlefield environment on threat COAs considering the specific threat your command is facing. Following are some examples to consider:

- Threat vehicles may have different values than the friendly vehicles you are used to in terms of mobility, optical systems, and so forth.
- The threat may have an organic capability that undermatched or overmatches your unit. If the threat is attacking without dismounted infantry, do not waste time identifying infiltration lanes. Likewise, a threat unit with exceptional bridging capabilities will be less affected by river obstacles.
- Bear in mind that weather will affect threat equipment differently than US equipment. Examples: An AK-47 is more resistant to moisture than an M-16. Likewise, fog will affect US thermal sights less than it will affect vehicles with optical sights only.

- Remember that "other characteristics" may sometimes influence threat actions more than terrain or weather considerations. Remember, also, to account for the cultural bias the threat operates within. They will evaluate the same legal, political, economic, and demographic aspects in a completely different manner than US personnel would.

The bottom line is to evaluate the battlefield completely from the perspective of the threat. Remember to express this evaluation in terms of COAs, not detailed descriptions of the analytical factors that led to the conclusions.

Focus the commander on concluding statements such as, "Sir, the battlefield environment best supports insurgent attacks on US and host nation (HN) forces near Daleytown. The next best place for their operations is Elkinsville." Be prepared to back these conclusions with the detailed analysis prepared in the previous steps.

Communicate the final conclusions from the description of the battlefield environment in written reports such as the analysis of the AO or the intelligence estimate. Distribute the graphic products developed during the analysis and evaluation as needed to support the remainder of the staff and other commands in their own IPB and planning efforts.

Evaluate the Threat

What Is It?

Definition:

The determination of threat force capabilities and the doctrinal principles and TTP threat forces prefer to employ.

An Example:

While planning a contingency show of force operation, a J2 directs the Joint Intelligence Center (JIC) to study the decisions on record of the targeted country's dictator. As a result of this research, the intelligence center produces a model of how the dictator makes decisions, with special emphasis on his tendencies during political crises.

Meanwhile, the S2 of the brigade which will conduct the operation does his own evaluation of the threat. He evaluates his contingency area order of battle (OB) files and determines that the two threat brigades within the target area are equipped, organized, and trained well enough to be capable of offensive as well as defensive operations against the friendly brigade. He prepares threat models depicting the threat's normal offensive and defensive operations in built-up areas (the setting for the show of force operation).

Desired End Effect:

Know the enemy. Develop threat models which accurately portray how threat forces normally execute operations and how they have reacted to similar situations in the past. Know what the threat is capable of, given the current situation.

The threat model should include-

- Standard graphic control measures, such as boundaries.
- A description of typical tasks for subordinate units.
- An evaluation of how well the threat force is trained on the task.
- Employment considerations.
- A discussion of typical contingencies, sequels, failure options, and wildcard variations.

- An evaluation of the threat's strengths, weaknesses, and vulnerabilities, including an evaluation of typical HVTs.

So What?

Success Results In:

Threat COAs developed in the next step of IPB reflect what the threat is and is not capable of and trained to do in similar situations.

Consequences of Failure:

The staff will lack the intelligence needed for planning.

The threat will surprise the friendly force with capabilities that the G2/S2 failed to account for.

At the other extreme, the friendly staff may waste time and effort planning against threat capabilities that do not exist.

How To Do It:

- Update or create threat models:
  - Convert threat doctrine or patterns of operation to graphics (doctrinal templates).
  - Describe in words the threat's tactics and options.
  - Identify HVTs.
- Identify threat capabilities.

Each of these steps is discussed below.

Update or Create Threat Models

Threat models depict how threat forces prefer to conduct operations under ideal conditions. They are based on the threat's normal or "doctrinal" organization, equipment, doctrine, and TTP. Threat models result from a detailed study of the threat force. Ideally, you construct threat models prior to deployment. Even after deployment, however, continue to evaluate the threat and update the threat models as required.

Threat models consist of three parts:

- Doctrinal templates.
- Description of preferred tactics and options.
- Identification of type HVTs.

An effective technique for recording threat models is to use the target spreadsheet format (see Figure 2-10).

Each part of the threat model is discussed in detail below.

Doctrinal Templates:

Doctrinal templates illustrate the deployment pattern and disposition preferred by the threat's normal tactics when not constrained by the effects of the battlefield environment. They are usually scaled graphic depictions of threat dispositions for a particular type of standard operation, such as a battalion movement to contact, an insurgent ambush, or a terrorist kidnapping. Figure 2-11 shows one such doctrinal template.

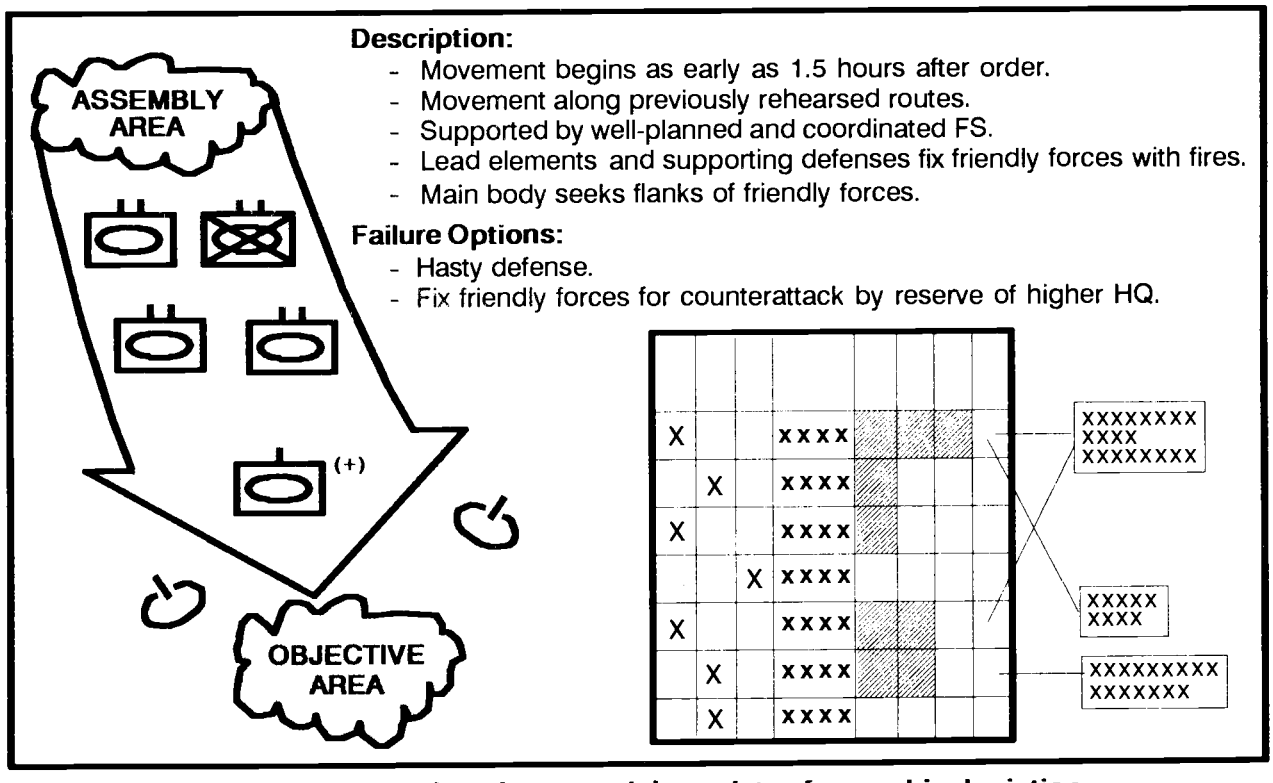

ASSEMBLY AREA
(+)
OBJECTIVE AREA
Description:
- Movement begins as early as 1.5 hours after order.
- Movement along previously rehearsed routes.
- Supported by well-planned and coordinated FS.
- Lead elements and supporting defenses fix friendly forces with fires.
- Main body seeks flanks of friendly forces.
Failure Options:
- Hasty defense.
- Fix friendly forces for counterattack by reserve of higher HQ.
XXXXXXXX XXXX XXXXXXXX
XXXXX XXXX
XXXXXXXXX XXXXXXX

Figure 2-10. A complete threat model consists of a graphic depiction, a description and identification of HVTs.

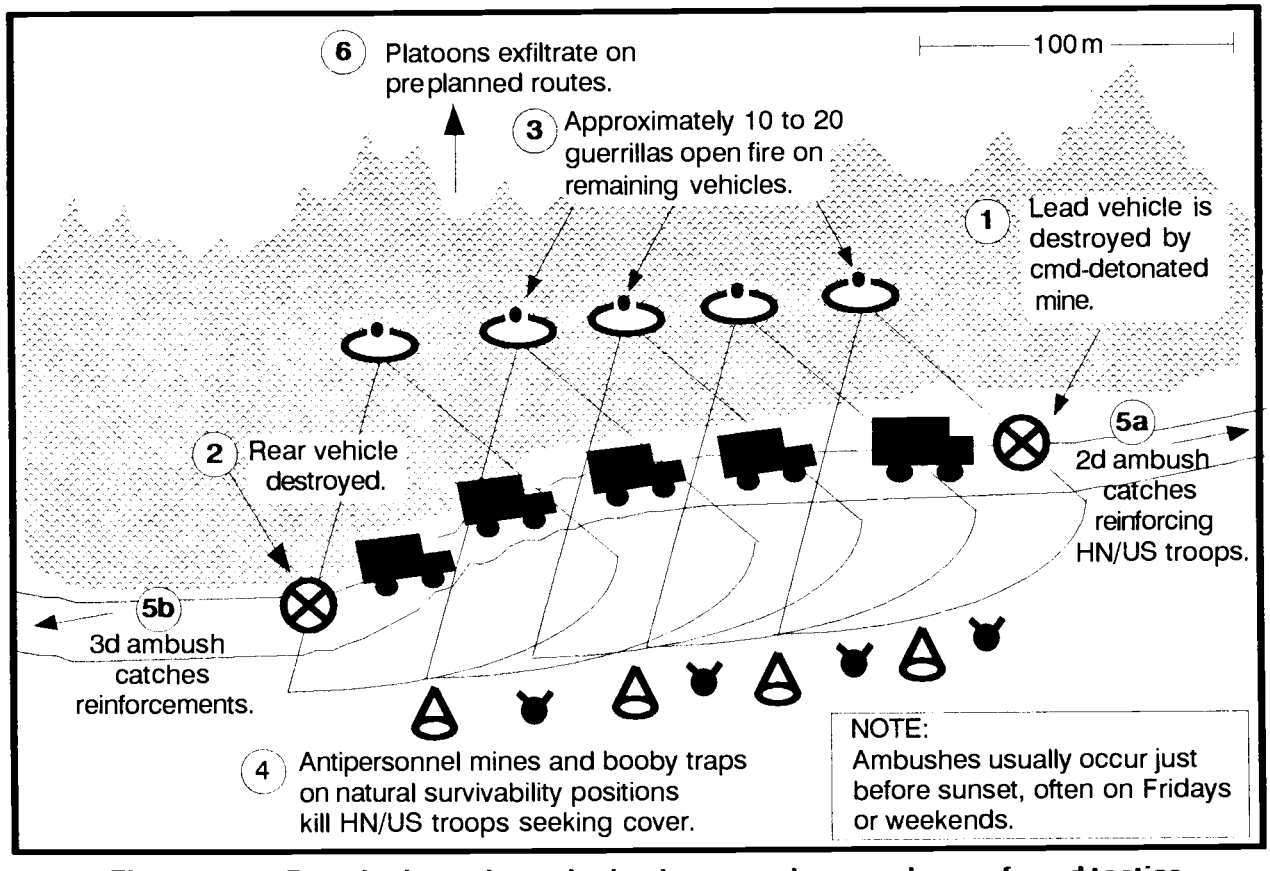

6 Platoons exfiltrate on preplanned routes.
100 m
3 Approximately 10 to 20 guerrillas open fire on remaining vehicles.
1 Lead vehicle is destroyed by cmd-detonated mine.
2 Rear vehicle destroyed.
5a 2d ambush catches reinforcing HN/US troops.
5b 3d ambush catches reinforcements.
4 Antipersonnel mines and booby traps on natural survivability positions kill HN/US troops seeking cover.
NOTE:
Ambushes usually occur just before sunset, often on Fridays or weekends.

Figure 2-11. Doctrinal templates depict the enemy's normal or preferred tactics.

Construct doctrinal templates through an analysis of the intelligence data base and an evaluation of the threat's past operations. Determine how the threat normally organizes for combat and how he deploys and employs his units and the various BOS assets. Look for patterns in task organization of forces, timing, distances, relative locations, groupings, or use of the terrain or weather. Focus on major elements as well as individual HVTs.

Even unconventional operations lend themselves to graphic depiction. For example, an evaluation of the data base might indicate that when robbing banks the threat always sends four guerrillas inside with at least two remaining outside. The four who move inside the bank usually take up positions at distinct locations within the bank. This type of information can easily be converted into a graphic representation, although not necessarily to a standard map scale.

Doctrinal templates can also portray the threat's normal organization for combat, typical supporting elements available from higher commands, frontages, depths, boundaries, engagement areas, objective depths, and other control measures. Whenever possible, convert these patterns into graphic representations such as overlays or sketches.

Doctrinal templates are tailored to the needs of the unit or staff section creating them. For example, a division G2 creates a template that differs in scope from that constructed by a battalion S2; the template constructed by an EW section differs drastically from that constructed by an air defense unit. An air defense doctrinal template, for example, would include a description of normal strike package composition, altitudes, time spacing between groups of aircraft, and so forth.

Some doctrinal templates consider the threat unit or force as a whole, while others focus on a single BOS, such as intelligence or fire support.

Description of Tactics and Options:
The threat model includes a description of the threat's preferred tactics. It addresses the operations of the major units or elements portrayed on the template and the activities of the different battlefield operating systems. It also contains a listing or description of the options available to the threat should the operation fail (branches), or subsequent operations if it succeeds (sequels).

Even if the threat's preferred tactics can be depicted graphically, the threat model includes a description. This allows the template to become more than a "snapshot in time" of the operation being depicted. It aids in mentally wargaming the operation over its duration during the development of threat COAs and situation templates.

The description should address typical tin-dines and phases of the operation (maneuver and support), points where units transition from one formation to another, and how each BOS contributes to the operation's success. Describe the actions of the supporting BOS in enough detail to allow the later identification of HVTs and HPTs. Since the target's value usually varies with its role in each phase of the operation, ensure that you examine each phase separately.

Like the template itself, you develop the description of the threat's tactics and options from an evaluation of his doctrine and past or current operations. Include a description of the branches and sequels normally available to or preferred by the threat should the depicted operation succeed or fail. For example, the threat might prefer to follow successful attacks with pursuit. Should an attack begin to fail, his preferred branches might include committing reserves, reinforcement, or shifting the main effort. Should the attack fail, his preferred sequel might be a hasty defense.

If the data base reveals any decision criteria that cause the threat to prefer one option over another, include that in the description. This information will aid in wargaming threat and friendly COAs, targeting, and deception planning.

Techniques:

- Start with the scheme of maneuver, then examine how each BOS "fits in" or provides support.
- Time-event charts can describe how the threat normally conducts an operation. For example, while it is difficult to depict a large scale air operation graphically, the time relationship between the various echelons and their normal composition can easily be described in a time-event chart, narrative, or matrix format.
- Marginal notations on the graphic template are an effective technique, especially when the notes are tagged to key events or positions on the template. For example, marginal notes might describe the insurgent's normal reactions to friendly reinforcements during their conduct of an ambush (see Figure 2-11).
- A BOS synchronization matrix depicts the threat's TTP in matrix form. See Chapter 3 for some examples.

Identification of Type HVTs:
Assets that the threat commander requires for the successful completion of the mission depicted and described on the template are HVTs.

Identify HVTs from an evaluation of the data base, the doctrinal template, its supporting narrative, and the use of tactical judgment. HVTs usually (but not always) fall within the non-maneuver BOS. Develop the initial list of HVTs by mentally wargaming and thinking through the operation under consideration and how the threat will use the assets of each BOS to support it. Identify any that are critical to the operation's success.

For example, while mentally wargaming an enemy air attack against friendly targets supported by a well prepared air defense system, it is logical to assume that the enemy will need a substantial air defense suppression package as part of the strike force. In such a case, threat aircraft commonly used in such a role become HVTs.

Identity assets which are key to executing the primary operation. Also identify any assets which are key to satisfying decision criteria or initial adoption of the branches and sequels listed in the description and option statements.

Determine how the threat might react to the loss of each identified HVT. Consider his ability to substitute other assets as well as the likelihood of adopting branches to the operation.

After identifying the set of HVTs, rank order them with regard to their relative worth to the threat's operation and record them as part of the threat model. An HVT's value usually varies over the course of an operation. Identify any changes in value by phase of the operation and make the necessary annotations.

As you identify key assets, group them into one of the 13 categories used to develop target sets. These 13 categories are—

- Command, control, and communications (C^3).
- Fire support (includes target acquisition assets, ammunition, aircraft, fire direction control, and others).

- Maneuver.
- Air defense (includes radars, processing centers, and headquarters).
- Engineer.
- Reconnaissance, intelligence, surveillance, and target acquisition (RISTA).
- NBC (includes support elements and weapons).
- Radio electronic combat (REC) or EW assets.
- Bulk fuels (storage and refueling assets).
- Ammunition storage sites and distribution points.
- Maintenance and repair units (includes collection points and mobile repair facilities).
- Lift.
- LOCs (roads, bridges, railheads, transloading facilities, airfields, choke points, others).

In a pinch, you can annotate the identified HVTs in the margins of the doctrinal template. When fully developed, HVT evaluations take the form of target relative value matrices (see Figure 2-12).

Target value matrices give a measure of the relative worth of targets, the rationale behind an attack on each type of target, and the resulting effects on the operation. See FM 6-20-10 for a complete discussion.

As always, tailor IPB to your needs by concentrating on potential HVTs important to your command or mission area. For example, an ADA unit's evaluation of HVTs might concentrate on distinguishing between the relative HVT worth of one type of aircraft over another. A CIAS might focus on the relative HVT worth of one type of intelligence collector or discipline over another.

Additional Considerations:

- Use all available intelligence sources to update and refine threat models. The most useful are the OB files. OB tiles contain the details which allow you to reach conclusions about the threat's operations, capabilities, and weaknesses. The OB factors that structure the OB files are—
  - Composition.
  - Disposition.
  - Strength.
  - Tactics or modus operandi (including habitual operating areas for unconventional warfare [UW] forces, gangs, insurgences, and so forth).
  - Training status.
  - Logistics.
  - Effectiveness.
  - Electronic technical data.
  - Miscellaneous data (personalities, pseudonyms, other).

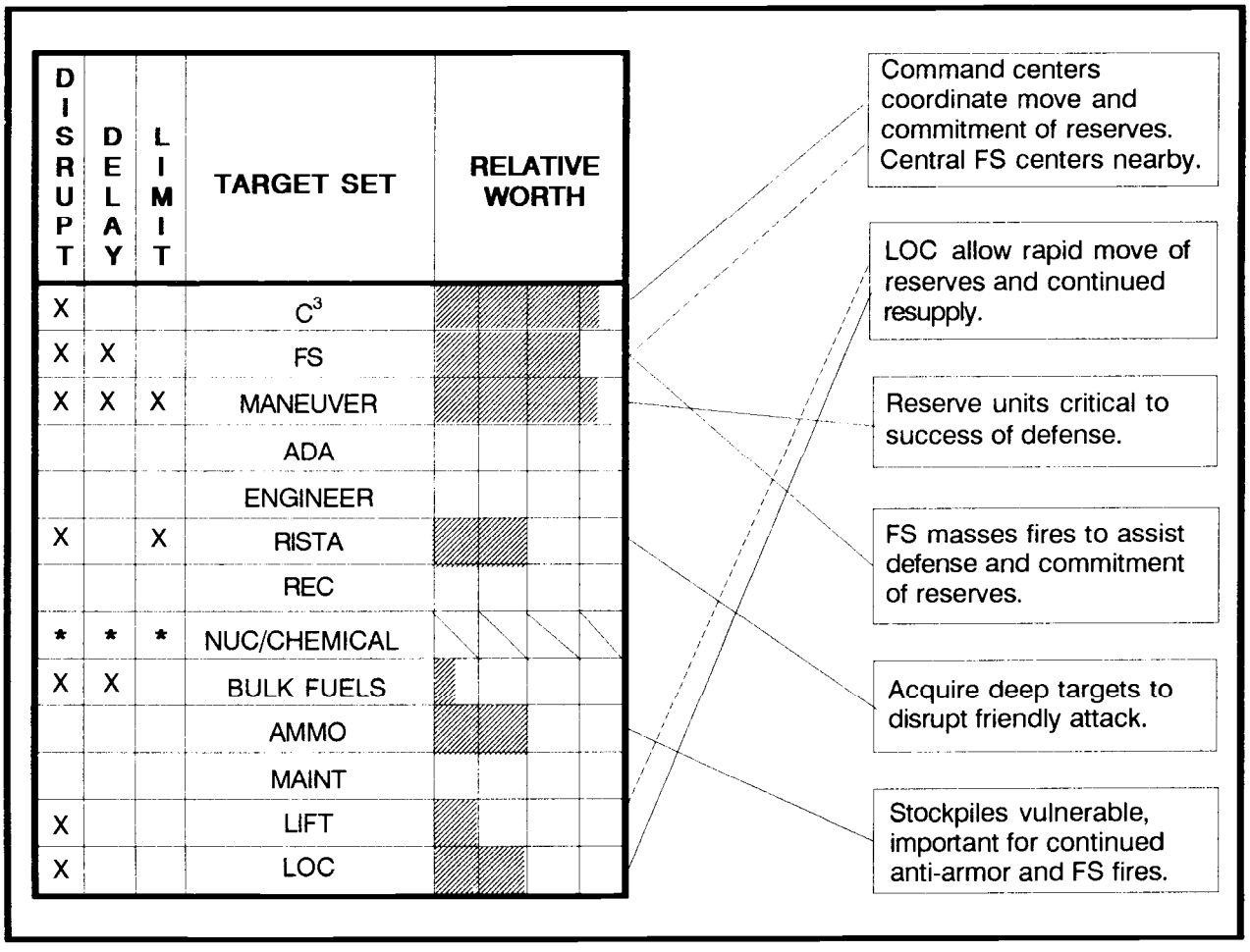


Figure 2-12. A complete threat model identifies HVTs.

- Create an OB file for each threat unit you are concerned with. Comparing the doctrinal norm with the files on each unit will indicate that most vary from the standard. Types of equipment as well as organization and training status may differ. As much as possible, the threat models should portray the specific units you are evaluating, not just the doctrinal norm.
- As time permits, continuously update the OB files as you develop intelligence during the processing phase of the intelligence cycle. Do not wait until staff planning begins to conduct the analysis. A common technique is to maintain a set of threat models under the "tactics" or "modus operandi" tab of each OB tile.
- Consider the various OB factors and their relationship when conducting the evaluation and updating the threat models. For example, how do direct fire weapon ranges and the threat's preferred size and location of engagement areas and battle positions relate?
  - If he increases his direct fire weapons system range, will he move his engagement areas farther from his battle positions, or make the engagement areas larger?
  - If he improves the range of his artillery systems will he employ them farther to his own rear, or use the extra range to engage deeper targets?

    - If his air defense capability improves, will he reduce the number of ADA assets in each unit?

- The OB factors are not independent of each other; they are closely related—consider them as a whole. For example, changes in training status, command personality, strength, or any other of the OB factors may affect the tactics of a unit at a given time.
- The OB factors form a framework for evaluation of any force, not just those that are strictly military. For example, when considering composition during a counter-drug operation, you might include an analysis of extended family ties of suspected traffickers. In evaluating an insurgent force, you would include an analysis of the insurgent political structure and its relationship to the military elements.
- Tailor evaluation of the OB factors to your unit needs. For example, an aviation unit's evaluation of composition would focus more heavily on those units that contained air defense assets. lts evaluation of equipment would focus on the vulnerabilities of likely threat targets as well as the technical characteristics of the threat's air defense systems.
- Consider not only the threat's physical capability based on organization and equipment strength but also his normal modus operandi, tactical doctrine, and state of training. This requires an understanding of the art and science of war as well as current knowledge of the threat. Ensure that you update the historical data bases with current observations whenever possible. For example, in scenario 3 of Chapter 3, the S2 uses three reports of recent insurgent ambushes to create a threat model depicting an insurgent ambush (see Figure 3-3-12).
- Mentally wargame the operation through to its completion. Do not stop at initial deployment of threat forces or initial contact with friendly forces.
- Rely on staff experts for help. The staff aviation officer, for example, probably knows a great deal about threat air and air defense operations.
- A useful technique in understanding how threat forces conduct operations is to first gain an understanding of how your own force conducts them. Then compare and contrast the threat's normal approach to the same operations. The OB factors form the framework for this evaluation. Another useful framework is the BOS.
- For a full discussion of the analytical techniques used in constructing threat models, see FMs 34-3, 34-7, 34-40(S), and 34-60.

Identify Threat Capabilities

Threat capabilities are the broad COAs and supporting operations which the threat can take to influence the accomplishment of the friendly mission. They take the form of statements, such as—

- "The enemy has the capability to attack with up to 8 divisions supported by 170 daily sorties of fixed-wing aircraft."
- "The enemy can establish a prepared defense by 14 May."
- "The enemy has the ability to insert up to 2 battalions of infantry in a single lift operation."
- "The drug smugglers have the capability to detect the radars used at our observation posts."
- "The threat can conduct up to three separate smuggling operations simultaneously."

- "The protesters can effectively block traffic at no more than 7 different intersections."

There are generally four tactical COAs open to military forces in conventional operations:

- Attack.
- Defend.
- Reinforce.
- Conduct a retrograde.

Each of these broad COAs can be divided into a variety of more specific COAs. For example, an attack may be an envelopment, a penetration, or other variations of an attack. A retrograde movement may be a delaying action, a withdrawal, or a retirement.

Other capabilities include support to broad COAs or specific types of operations. Examples of these types of capabilities are—

- Use of NBC weapons.
- Use of supporting air assets.
- Intelligence collection.
- EW.
- Engineering operations.
- Air assault or airborne operations.
- Amphibious assaults.
- Riverine operations.
- Psychological operations (PSYOP).
- Deception operations.

At other levels of war and during operations other than war you will consider other types of operations and broad COAs. In any case, start with the full set of threat models and consider the threat's ability to conduct each operation based on the current situation.

Most situations will not present the threat with the ideal conditions envisioned by his doctrine and TTP. He will usually be under-strength in terms of personnel or equipment. He may be short of logistical support. He may not enjoy air superiority. His troops may be inexperienced or poorly trained. As a result, the threat's actual capabilities usually will not mirror the ideal capabilities represented by the complete set of threat models. For example:

- The threat's doctrine may call for penetration attacks when possible. Your evaluation of his current strength, however, may indicate that the threat lacks the force ratio he normally considers adequate for a penetration attack.
- A terrorist group's normal tactics may call for the use of car bombs or similar devices to tie down emergency services while they conduct raids in other parts of town. Your evaluation of the threat's current logistics status, however, might indicate a critical shortage of explosive materials.

Additional Considerations:

- Use all available intelligence sources in the evaluation of the threat's current situation. Focus on the *effects* each incident or fact has on threat capabilities rather than simply enumerating details.
- Use the OB files for the particular threat force you are evaluating. Most forces differ from the ideal portrayed in threat doctrine or tables of organization and equipment (TOE). They may be equipped or organized differently, train for special missions, or have a particular record of combat experiences that give them a unique set of capabilities.
- In addition to identiying actual threat capabilities, the evaluation may identify additional threat strengths or vulnerabilities caused by the current situation. Ensure you incorporate them into the threat models, the intelligence estimate, and the threat COAs you develop in the next step of the IPB process.
- Consider the threat's ability to operate in darkness or adverse weather. This is more than the technical capability of selected items of threat equipment. For example, the threat's tank fleet may be equipped with the latest in night vision devices but the supporting infantry and other arms may not be.
- Also consider training levels. A force that frequently trains in night combat may have a better capability for such operations than a better equipped force that seldom trains at night. A force that has never trained in large scale troop movements may have a limited capability to conduct large offensive maneuvers.
- Consider the time element when evaluating capabilities. For example, the threat's forces may be currently dispersed to the point where he is not capable of offensive action. Given time, however, he can mass his forces. Similarly, the threat's current logistical stockage may permit offensive operations for only a limited amount of time before his stockpiles are exhausted.
- When time or some other factor is a critical element in a threat capability, ensure that you state it explicitly. For example:
    - "The enemy has the capability to attack to seize objectives no deeper than the line SOCHATON-MESSVILLE due to insufficient fuel reserves."
    - "The enemy has the capability to attack after repositioning major elements of the IV Army. Current dispositions preclude an attack before 9 July."
    - "The insurgents will have the manpower they need to conduct offensive action once the harvest is completed."

Do not limit the threat models and evaluation of capabilities strictly to military forces of the threat. Student rioters during a noncombatant evacuation (NEO) operation, for example, are a threat to the friendly mission. Evaluate them using all the techniques described in this section.

Like all other parts of the IPB process, tailor the evaluation to your particular needs. A CIAS, for example, focuses on the threat's intelligence collection capabilities, and levels I and II threats. Signal units focus on the ability of the threat to disrupt friendly communications.

Disseminate the results of evaluating the threat as widely as possible. This allows other staff sections and units to include them in their own IPB process. For example, the doctrinal

templates produced by a division will be refined by subordinate battalions to include a greater degree of detail. Templates produced by a G2 or S2 section will be modified by other staff sections, possibly to highlight specific BOSs in more detail, such as air defense assets.

In addition to distributing threat models, disseminate the results of evaluating the threat's capabilities, strengths, and vulnerabilities. The traditional means of disseminating the evaluation is the intelligence estimate, but always use the means best suited to the situation. The graphics that make up the threat model might best be delivered by courier. You can also deliver other parts of the evaluation by voice communications or over automated systems.

For a full discussion of the analytical techniques used in evaluating the threat, refer to FMs 34-3, 34-7, 34-40(S), and 34-60.

Determine Threat Courses of Action

What Is It?

Definition:

The identification and development of likely threat COAs that will influence accomplishment of the friendly mission.

An Example:

A Boer S2 tells his commander: "Sir, the enemy platoon leader's likely objective is to retain control of the only crossing point suitable for wheeled traffic over the Silliaasvogel River. He can defend the crossing, known as Duffer's Drift, with his 50 soldiers in any one of the following ways:

(1) "He can leave it undefended until tomorrow (being inexperienced and thinking that we will not arrive until the next day).

(2) "He can dig his platoon into a small enclosure just on the other side of the drift. A variant of this COA would be for him to establish a trenchline astride the main road.

(3) "He can occupy and fortify the Kraal village that overlooks the drift.

(4) "He can occupy the riverbed itself with only a small outpost in the Kraal village. This goes against every canon in British doctrine; however, we must consider this COA because it is so dangerous to the accomplishment of our mission.

"Sir, I think the platoon leader will adopt one of these COAs, in order of probability as I gave them. We need to conduct reconnaissance of the riverbed and the Kraal in order to find out which of these COAs he has chosen."

(Note: "The Defence of Duffer's Drift," by MC Sir Ernest Swinton, is a classic vignette illustrating the proper use of tactics, IPB, and the practical application of doctrine.)

Desired End Effect:

Replicate the set of COAs that the threat commander and staff are considering.

Identify all COAs that will influence the friendly command's mission.

Identify those areas and activities that, when observed, will discern which COA the threat commander has chosen.

We cannot count on air superiority during the opening stages of the conflict and, therefore, must pay special attention to the threat's air support capabilities (Figure 3-2-6). Evaluation of the threat model indicates we can expect up to 14 tighter-bomber sorties against targets in the brigade's sector each day. We extract the appropriate doctrinal template from the threat model (Figure 3-2-7).

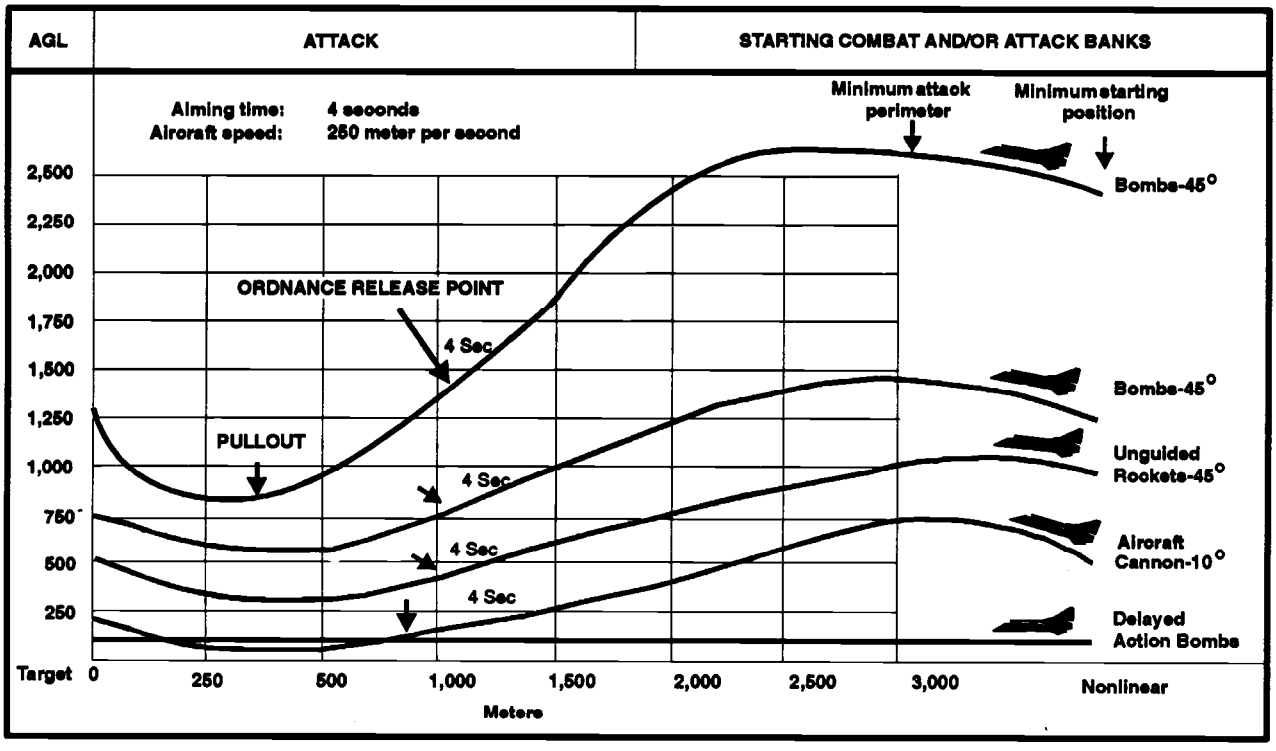


Figure 3-2-6. Doctrinal template of fighter-bomber employment.

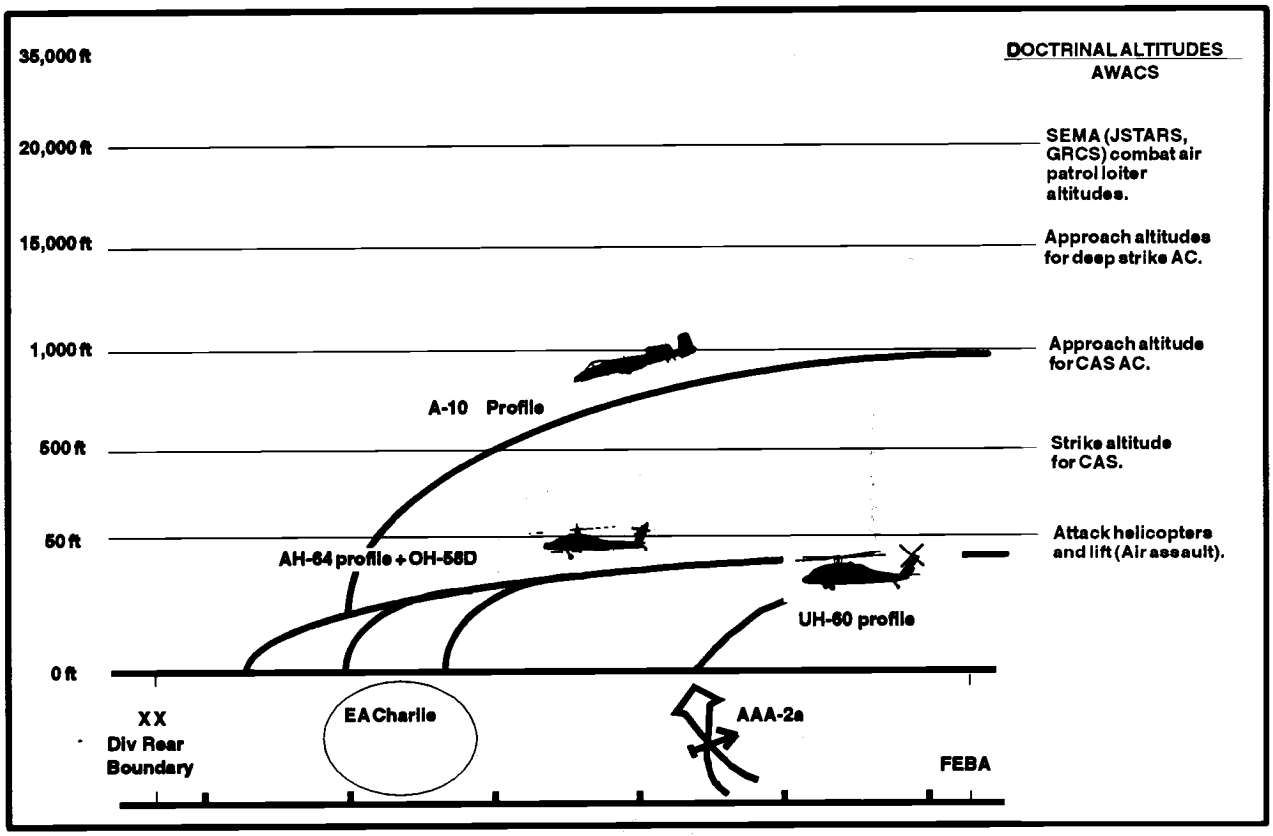


Figure 3-2-7. Altitude profile for AAA-2.

After studying the coordinates registers, time pattern analysis worksheets and the associated intelligence reports, the analysts realize that the insurgent techniques for conducting ambushes have evolved over time. Each operation is more sophisticated than those that preceded it as the insurgents learn from their mistakes. To reflect the most current "standard" techniques, the section prepares doctrinal templates. The doctrinal template at Figure 3-3-13 shows the section's best assessment of the current procedures used by the insurgents during ambushes.

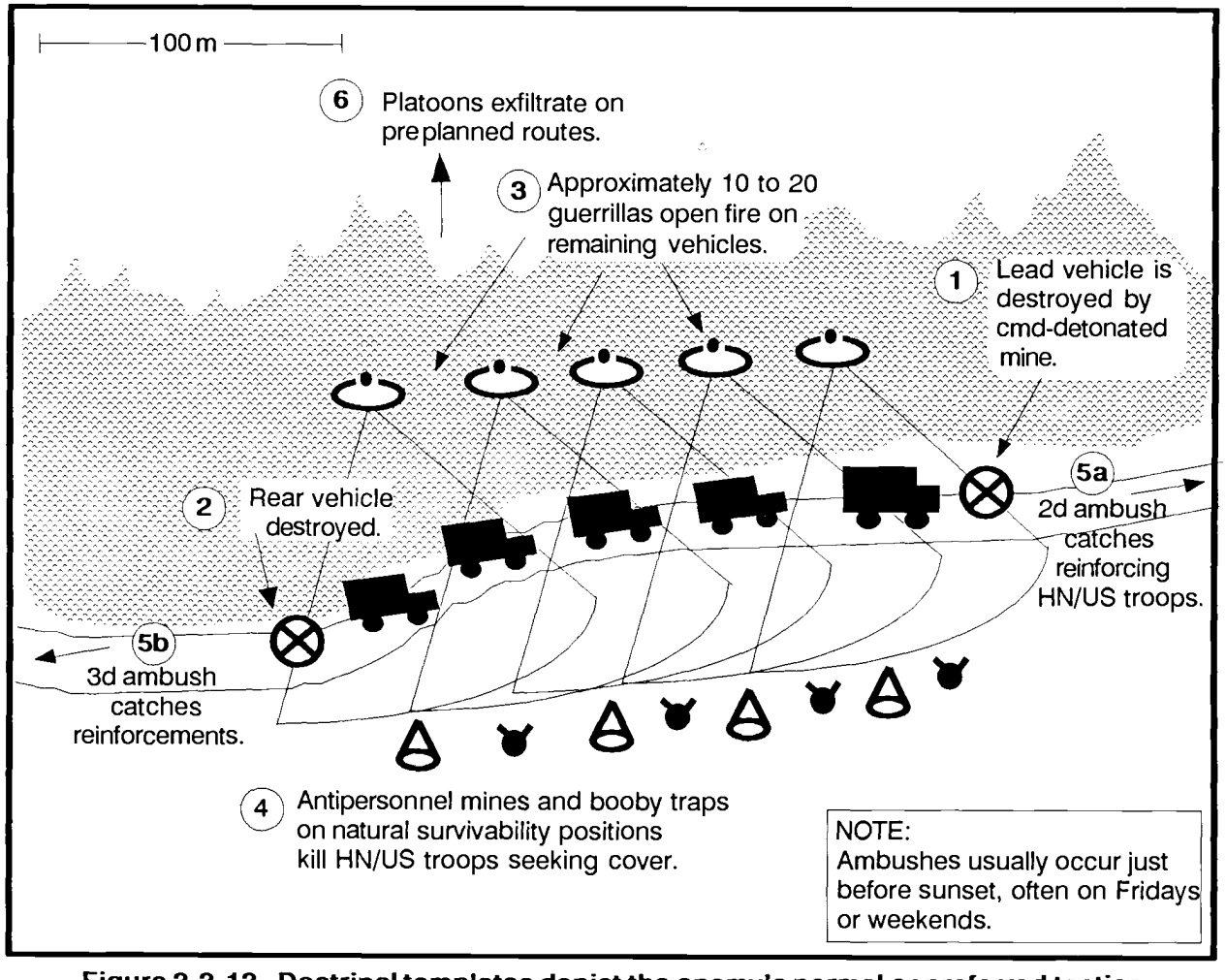

100 m
6 Platoons exfiltrate on preplanned routes.
3 Approximately 10 to 20 guerrillas open fire on remaining vehicles.
1 Lead vehicle is destroyed by cmd-detonated mine.
2 Rear vehicle destroyed.
5a 2d ambush catches reinforcing HN/US troops.
5b 3d ambush catches reinforcements.
4 Antipersonnel mines and booby traps on natural survivability positions kill HN/US troops seeking cover.
NOTE:
Ambushes usually occur just before sunset, often on Fridays or weekends.

Figure 3-3-13. Doctrinal templates depict the enemy's normal or preferred tactics.

The section does the same for insurgent raids. The result is a doctrinal template that depicts current "standard" techniques for raids on facilities or installations (Figure 3-3-14).

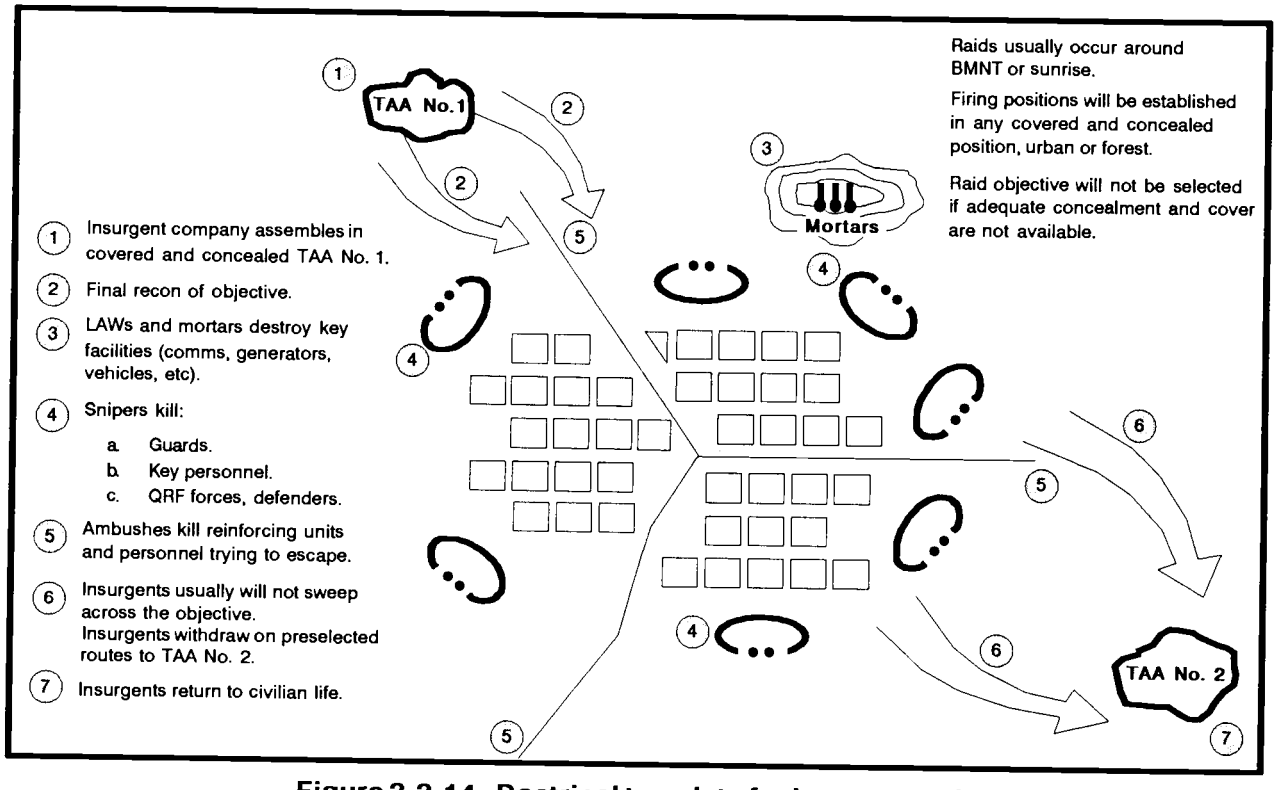

Raids usually occur around BMNT or sunrise.
Firing positions will be established in any covered and concealed position, urban or forest.
Raid objective will not be selected if adequate concealment and cover are not available.
1 Insurgent company assembles in covered and concealed TAA No. 1.
2 Final recon of objective.
3 LAWs and mortars destroy key facilities (comms, generators, vehicles, etc).
4 Snipers kill:
a. Guards.
b. Key personnel.
c. QRF forces, defenders.
5 Ambushes kill reinforcing units and personnel trying to escape.
6 Insurgents usually will not sweep across the objective. Insurgents withdraw on preselected routes to TAA No. 2.
7 Insurgents return to civilian life.
TAA No. 1
Mortars
TAA No. 2

Figure 3-3-14. Doctrinal template for insurgent raid.

To study the Metropolanian threat the S2 section only received an 8-year-old Defense Intelligence Agency handbook, some sketchy reports on recent training exercises, and some educated assessments by analysts at the division and regimental levels. The battalion S2 integrated the results of his analysis of these products into the doctrinal template (Figure 3-3-15).

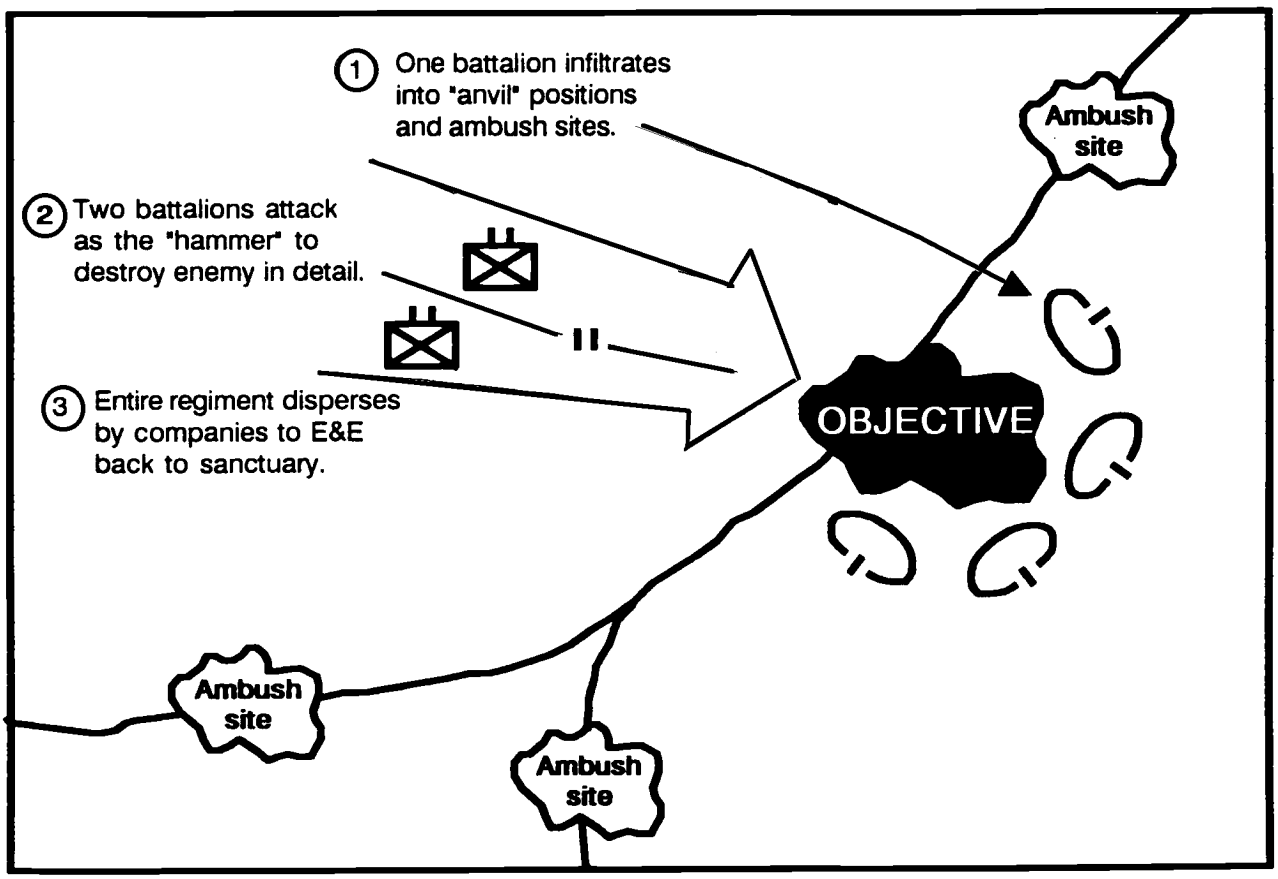

1 One battalion infiltrates into "anvil" positions and ambush sites.
2 Two battalions attack as the "hammer" to destroy enemy in detail.
3 Entire regiment disperses by companies to E&E back to sanctuary.
OBJECTIVE
Ambush site
Ambush site
Ambush site

Figure 3-3-15. Doctrinal template for Metropolanian attack.

DETERMINE THREAT COURSES OF ACTION

Having finished the initial three steps of IPB, the S2 section turned to determining enemy COAs. The section focused its efforts around a reliable and credible intelligence report that narrowed guerrilla targets down to incoming US Army personnel and government forces within areas sympathetic to the host nation.

The S2 prepared a situation template depicting likely insurgent COAs. He did this by integrating his IPB products depicting population status, availability of concealment and cover, and potential ambush sites with the threat model developed in the previous step.

In this case, the situation template takes the form of a key facilities and targets overlay, sometimes known as a "trap map," which shows likely targets for the insurgents (Figure 3-3-16). The S2 also included in the situation template the areas most likely to be used by an assembling insurgent company, and the infiltration routes between the objective sites and the assembly areas. This situation template also shows the safehouses that "wanted" personnel will probably use between insurgent operations.

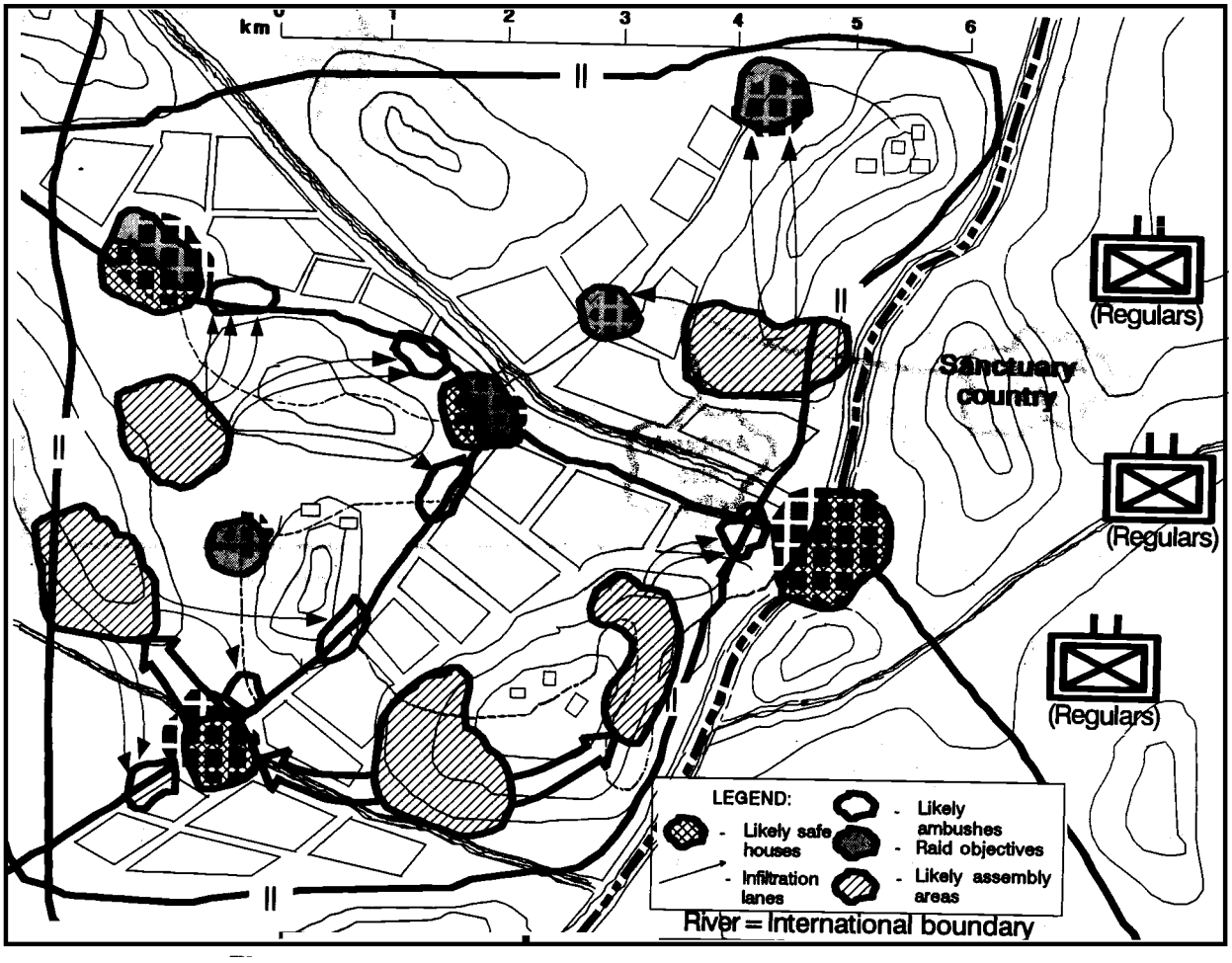


Figure 3-3-16. Situation template for insurgent ambushes.

Scenario Four: Noncomabatant Evacuation

Following intense political debate over an issue of regional politics, civil war has broken out on the island nation of Lilliput. With most of the island divided between them, the two rebel factions now confront each other--and the remaining government police forces-over control of the capital city of Gulliver (Figure 3-4). Fighting has died down while negotiations aimed at a peaceful transfer of the governmental center open. But all sides involved in the conflict patrol the fringes of the contested area, and there are still occasional armed clashes.

Hemmed in by the two warring factions, the otherwise ineffectual government forces have thus far managed to hold the capital city and safeguard the American citizens living there. The Lilliputian president has requested US evacuation of its citizens because he feels his forces will surrender to the first of the two factions to make a renewed assault on the city center, should negotiations collapse.

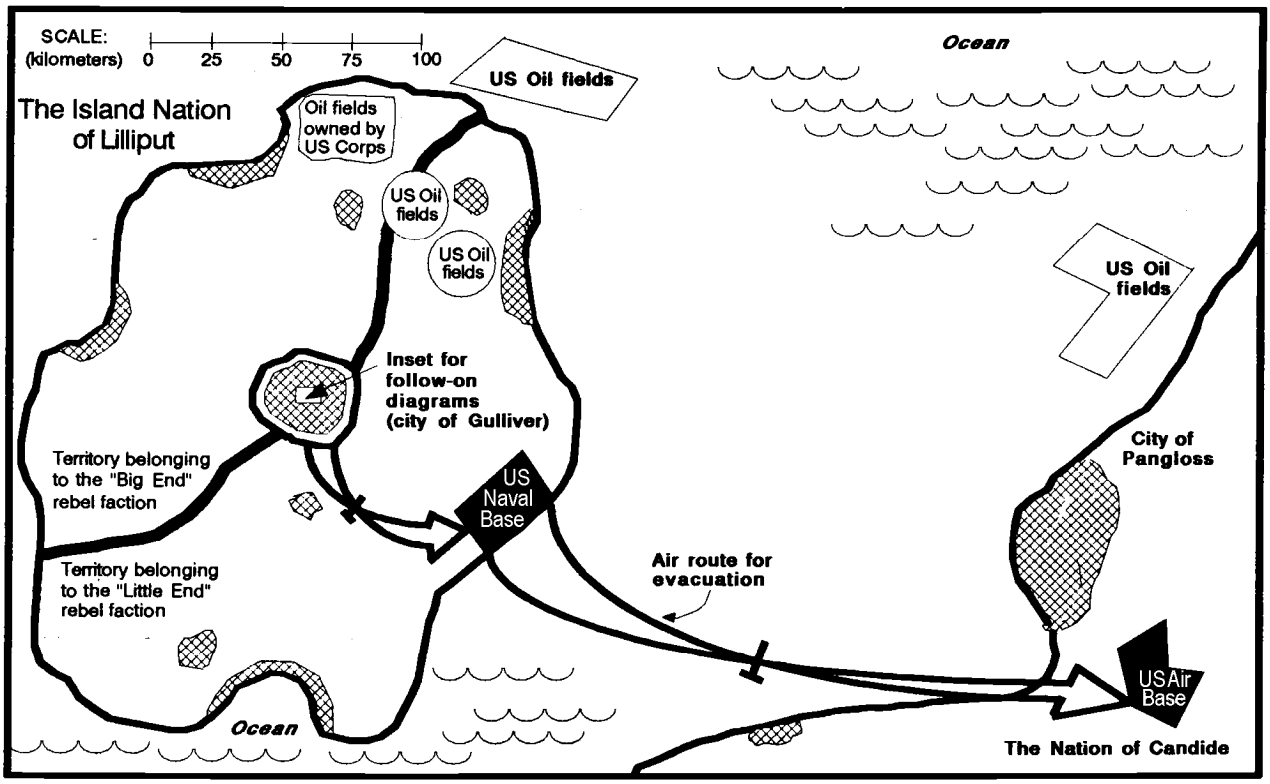

SCALE:
(kilometers) 0 25 50 75 100
The Island Nation of Lilliput
Oil fields owned by US Corps
US Oil fields
US Oil fields
US Oil fields
US Oil fields
Ocean
Inset for follow-on diagrams (city of Gulliver)
Territory belonging to the "Big End" rebel faction
Territory belonging to the "Little End" rebel faction
US Naval Base
Air route for evacuation
City of Pangloss
US Air Base
Ocean
The Nation of Candide

Figure 3-4. Scenario 4, general situation.

Our division has been ordered to evacuate American citizens from the capital of the island nation.

Neither of the two warring factions has displayed any openly anti-American sentiment. The greatest threat to the NEO is posed by the resumption of fighting between the two factions. There is also a risk of interference by groups of anti-American student activists from the city's university.

DEFINE THE BATTLEFIELD ENVIRONMENT

Our brigade (the 1st Brigade) is assigned responsibility for the center of the city. The brigade's boundary identifies the limits of its AO (Figure 3-4-1).

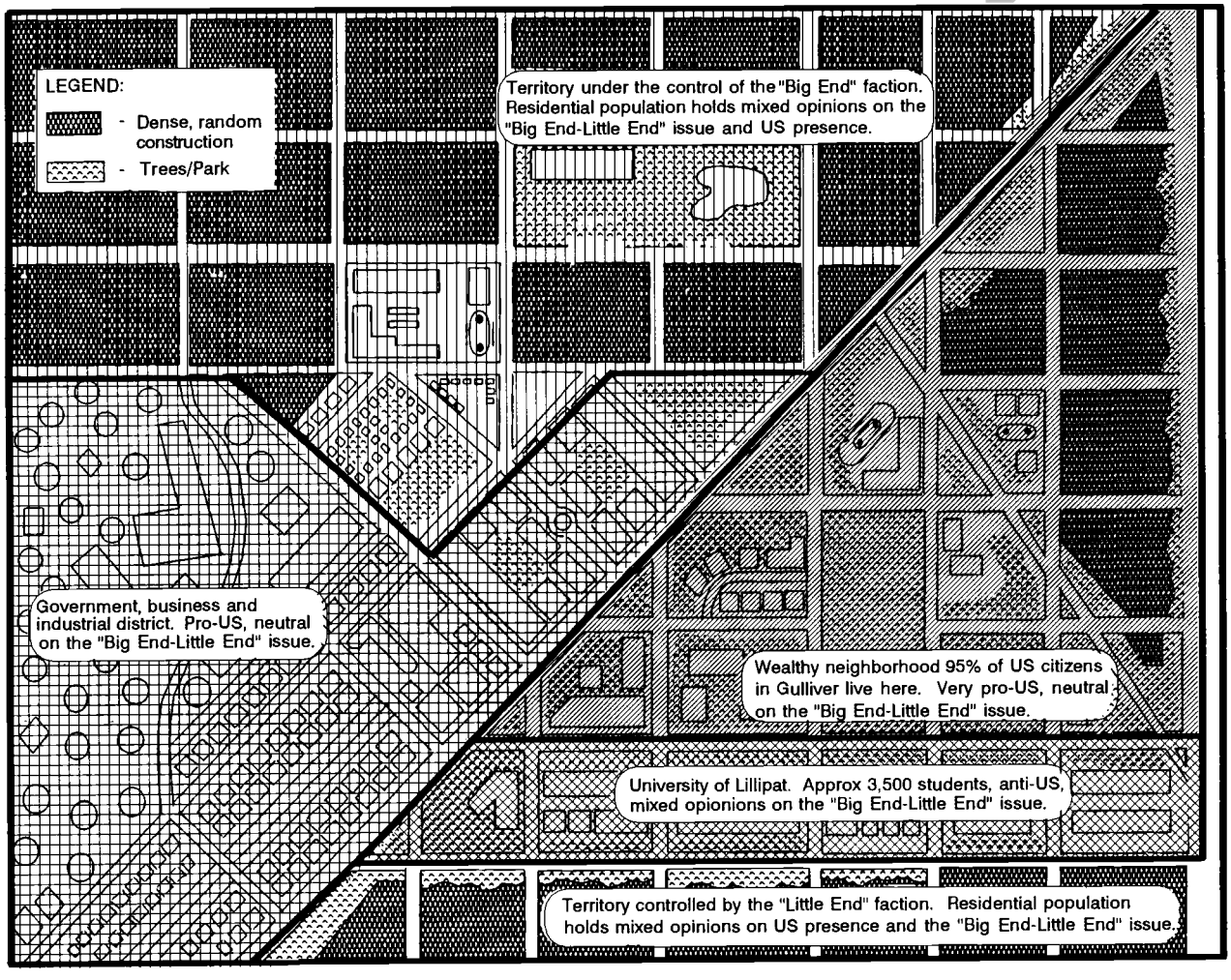

LEGEND:
- Dense, random construction
- Trees/Park
Territory under the control of the "Big End" faction. Residential population holds mixed opinions on the "Big End-Little End" issue and US presence.
Government, business and industrial district. Pro-US, neutral on the "Big End-Little End" issue.
Wealthy neighborhood 95% of US citizens in Gulliver live here. Very pro-US, neutral on the "Big End-Little End" issue.
University of Lillipat. Approx 3,500 students, anti-US, mixed opionions on the "Big End-Little End" issue.
Territory controlled by the "Little End" faction. Residential population holds mixed opinions on US presence and the "Big End-Little End" issue.

Figure 3-4-3. Population status overlay.

The AI includes our routes of ingress and egress in addition to any likely threats to the mission (Figure 3-4-2). Due to the nature of the operation and the battlefield environment, most of the city is included in the AI.

The nature of the operation requires us to include several other factors into the definition of the battlefield environment. The politics of the capital city and its populace will have considerable impact on the ease with which we can conduct the operation. The interactions between the two rival forces, and their interaction with US forces and diplomats, are also critical aspects of the definition of the battlefield environment. Should the negotiations occurring within the governmental center collapse, full-scale hostilities between the two rebel factions would likely resume, regardless of the risks to US citizens. Additionally, we must consider the role of the US country team, and the missions and activities of any friendly special operations forces that may be operating within the AI.

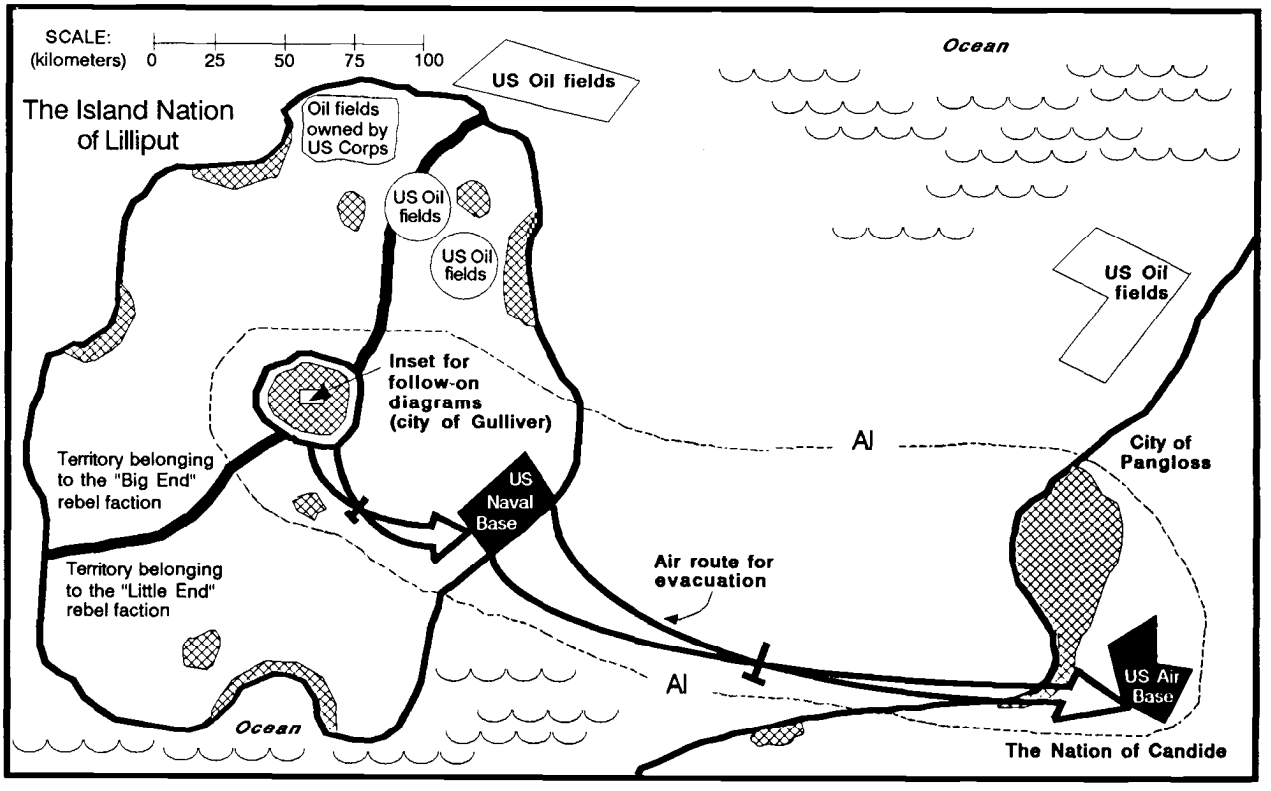


Figure 3-4-2. The area of interest.

DESCRIBE THE BATTLEFIELD'S EFFECT

The nature of the operation requires a focus on the populace of the city and their political affiliations. This form of population staus overlay allows us to identify areas where US citizens may be more or less at risk (Figure 3-4-3).

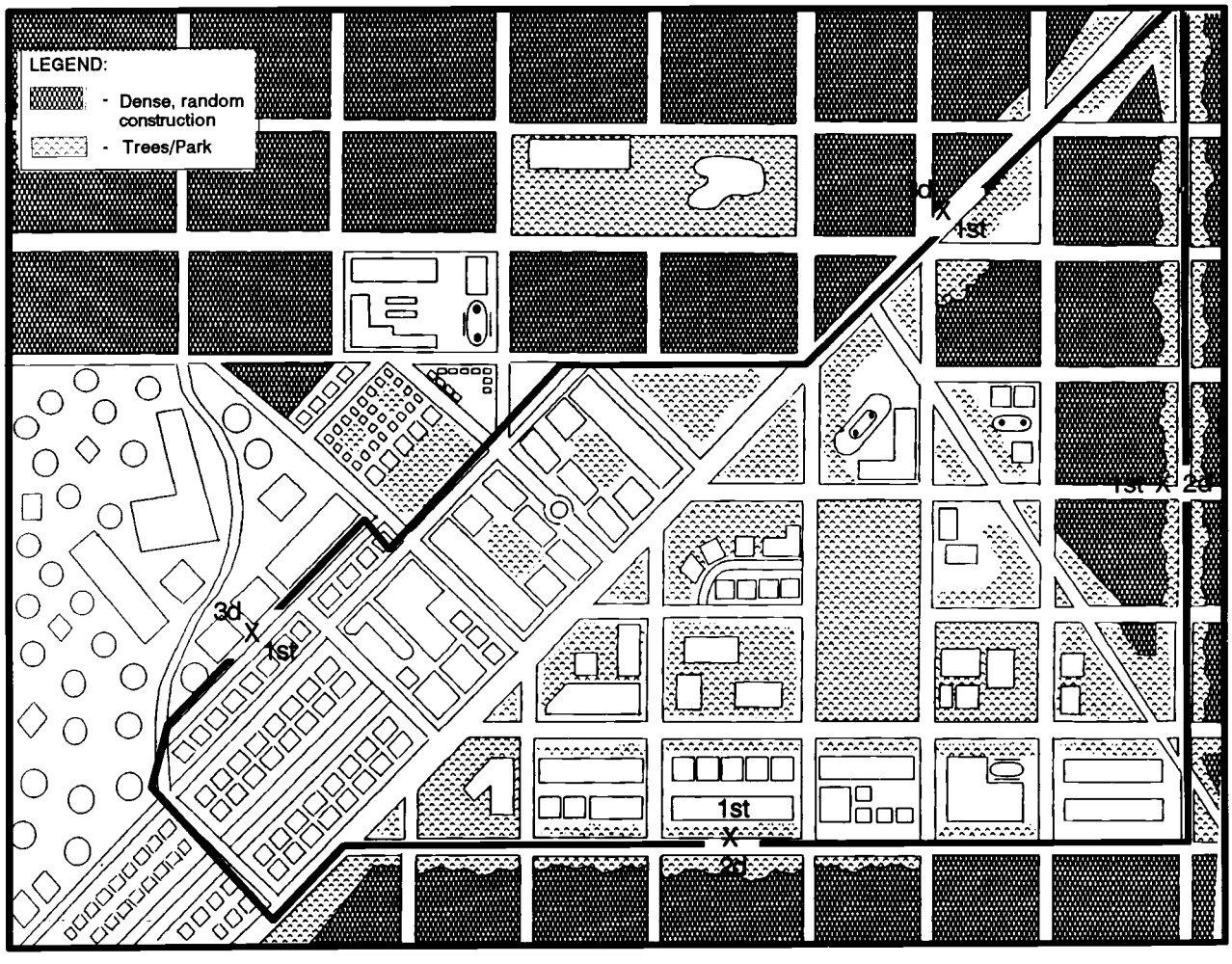


Figure 3-4-1. The area of operations.

We examine how the battlefield environment will affect our COAs as those of the "threat." We start with an evaluation of potential zones of entry (helicopter LZs [Figure 3-4-4]). With this we integrate an evaluation of areas suitable for use as assembly or "holding" areas for large numbers of civilians while they await evacuation.

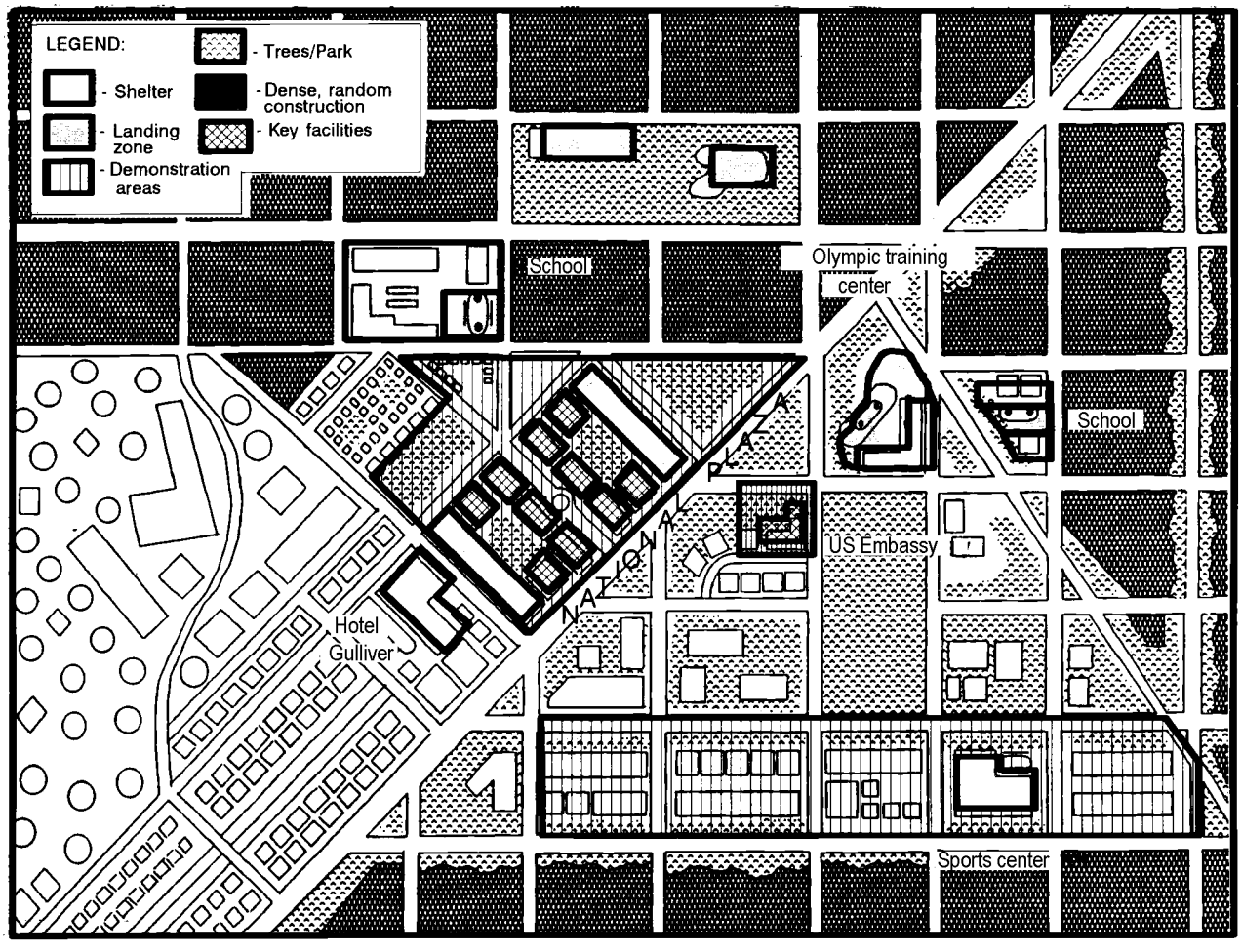


Figure 3-4-4. Zones of entry.

In urbanized terrain, the buildings themselves are the most dominating aspect of the terrain. We evaluate the type of building construction within our AI to determine its likely effects on operations (Figure 3-4-5). Building construction affects mobility, concealment and cover, and observation and fields of fire.

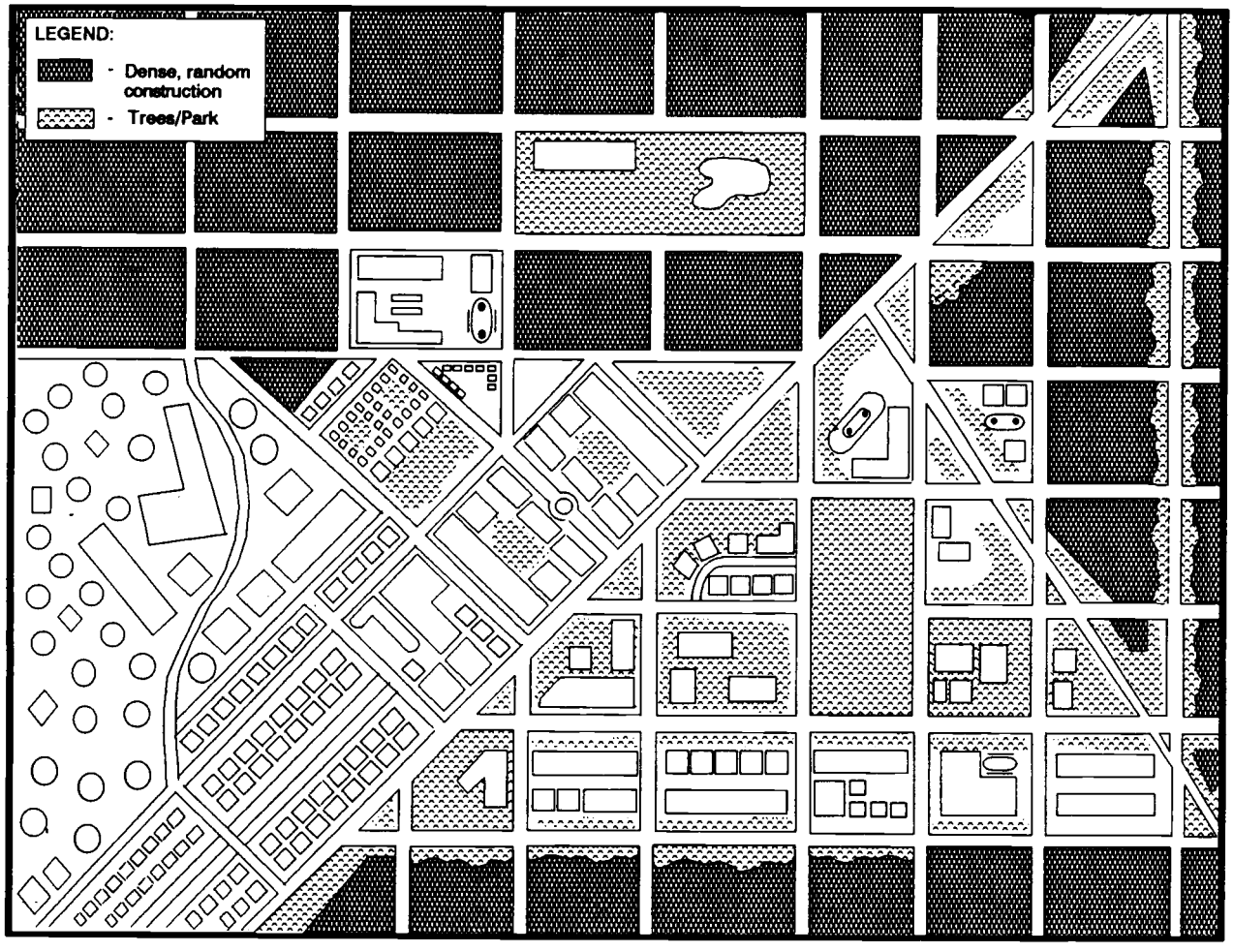


Figure 3-4-5. Building and construction types.

Although both rebel forces are now using roads to conduct their patrolling activities, we evaluate other suitable AAs. The areas with densely constructed woodframe buildings offer the best general AAs for dismounted infantry (Figure 3-4-6). The nature of the construction type in these areas may permit the rebels to form their own infiltration lanes by knocking holes in the walls of adjoining buildings; allowing them easy movement under cover. Additionally, the dense construction makes the use of rooftop AAs possible. Should full-scale hostilities break out, these areas maybe the focus of a rebel faction's operations aimed at securing control of areas under the control of the opposing faction.

Should the government's police forces collapse, other AAs might be used by either faction in a "dash" to seize the governmental center. These areas, such as the recreational parks, offer little cover but facilitate rapid movement by both dismounted infantry or the light trucks used by both rebel factions.

Control of the high-rise buildings in the city center will give our forces the best observation points within our AO and over the areas contested by the two rebel factions.

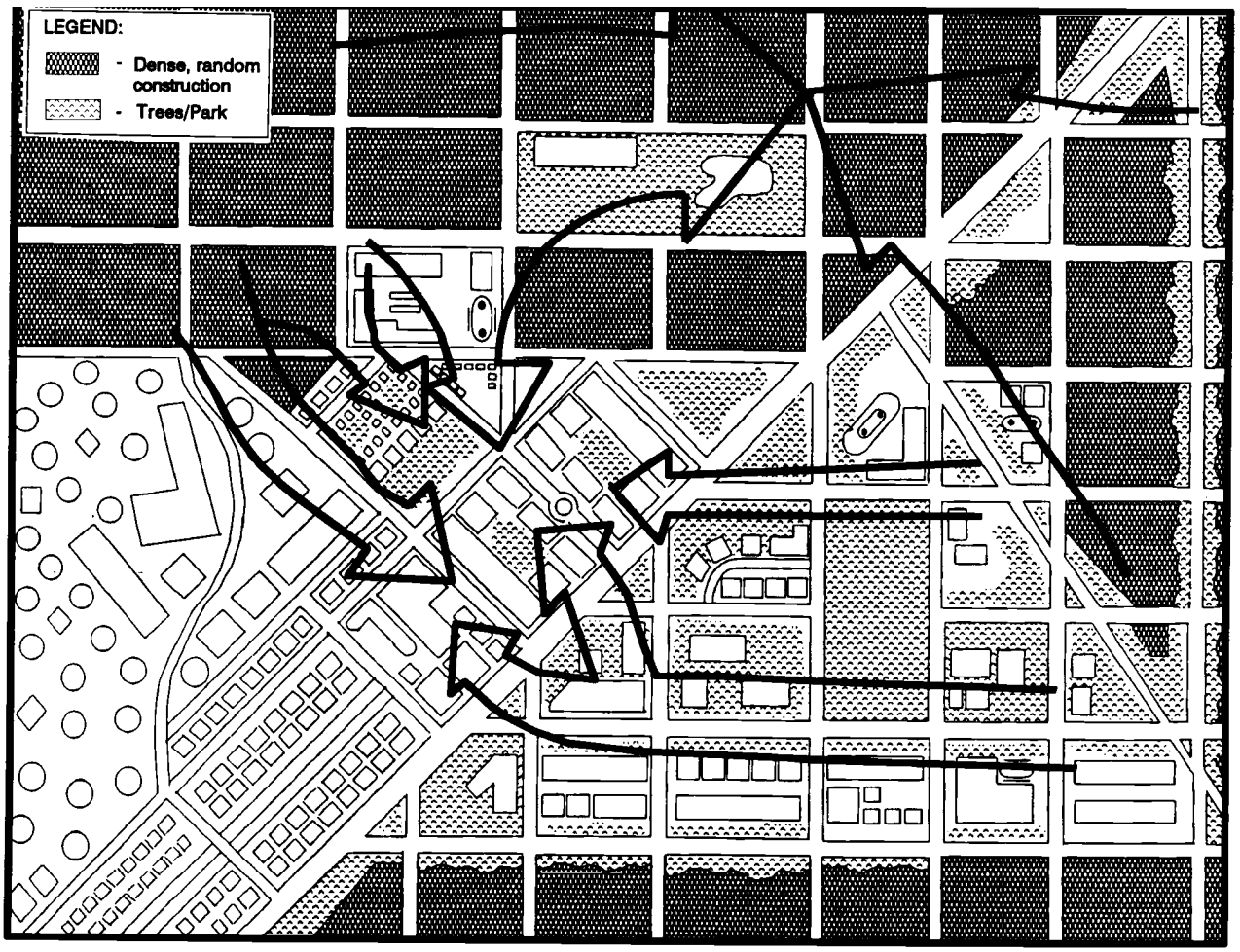


Figure 3-4-6. Avenues of approach.

Another consideration in urban terrain is the possible use of underground AAs provided by subway and other "under-street" utilities, such as sewer systems (Figure 3-4-7).

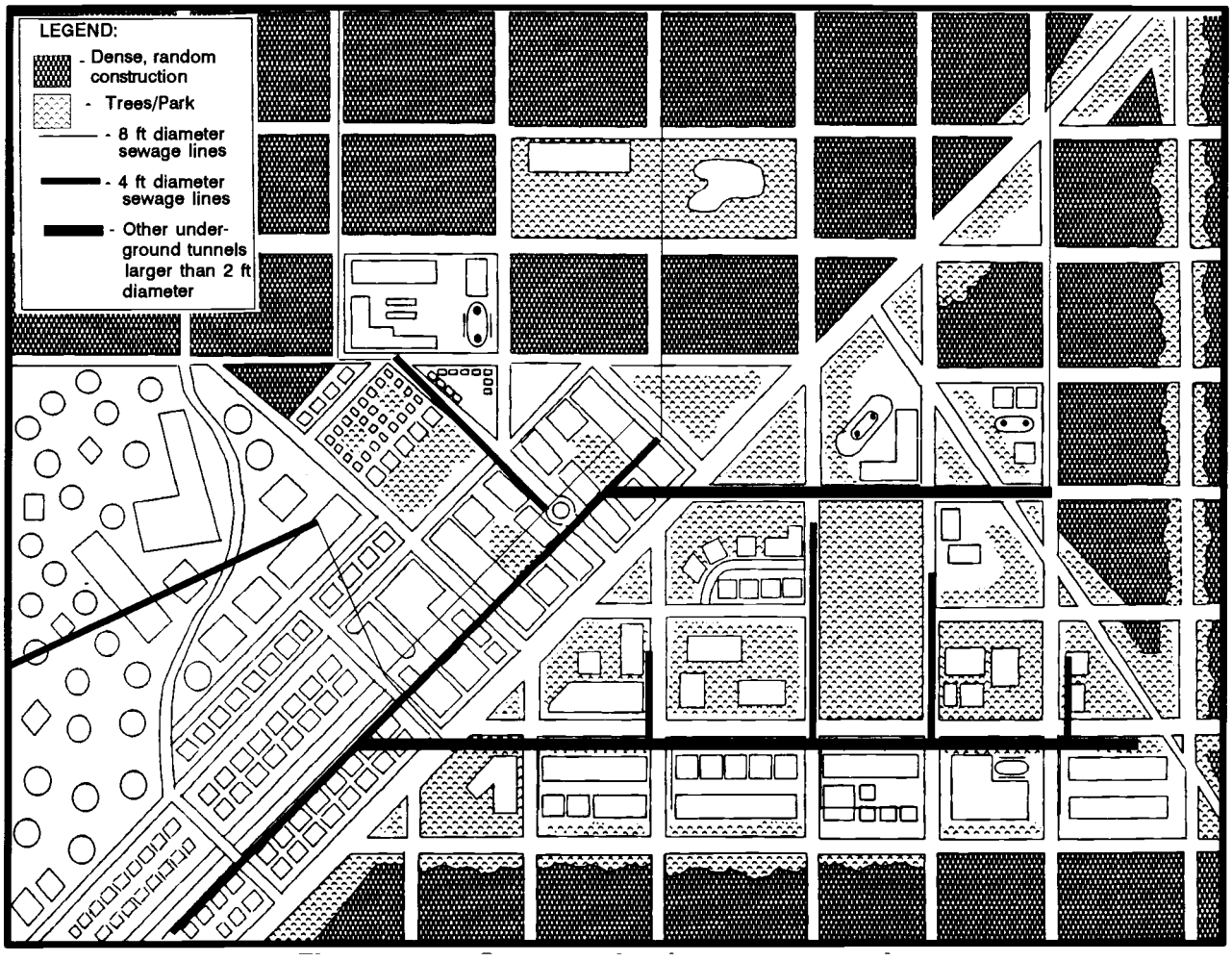

LEGEND:
- Dense, random construction
- Trees/Park
- 8 ft diameter sewage lines
- 4 ft diameter sewage lines
- Other underground tunnels larger than 2 ft diameter

Figure 3-4-7. Sewer and subterranean overlay.

EVALUATE THE THREAT

We begin with an examination of the little we know about the rebel forces and activist student organizations within the country (Figure 3-4-8).

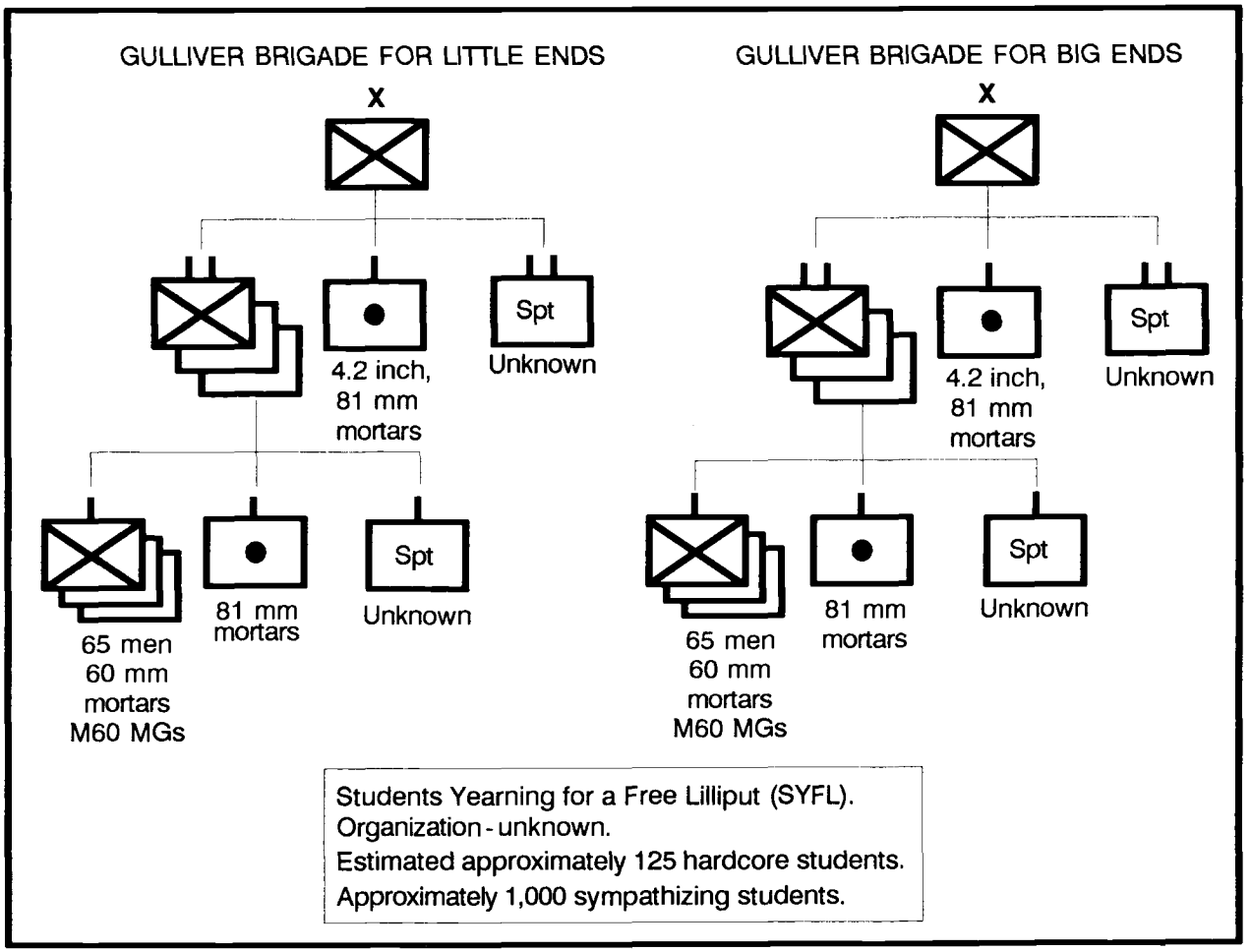


Figure 3-4-8. Enemy organizations.

In order to develop threat models, we examine the operations the rebel forces have conducted in the recent past (Figure 3-4-9). Although we use all available information, we focus on their operations within the capital city itself. This allows us to account for any peculiarities in their "normal" tactics caused by the political battle for control of the capital.

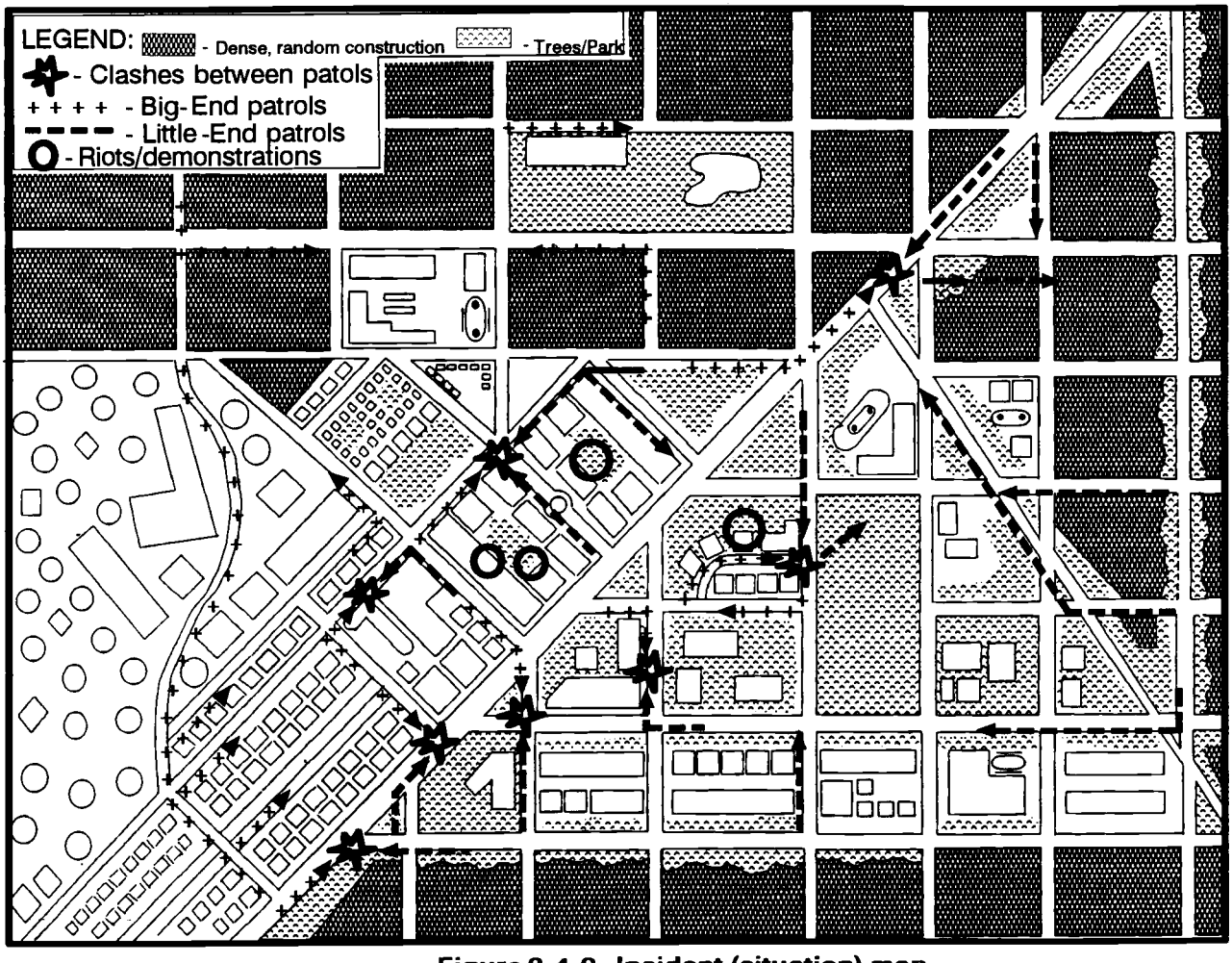


Figure 3-4-9. Incident (situation) map.

We also conduct a time-pattern analysis to determine the periods of highest threat to the evacuation operation. Patterns show up on the wheel as "funnel" shapes (Figure 3-4-10). Knowing the times of highest threat allows the commander to plan critical stages in the operation, such as the movement of noncombatants, for "low-threat" periods.

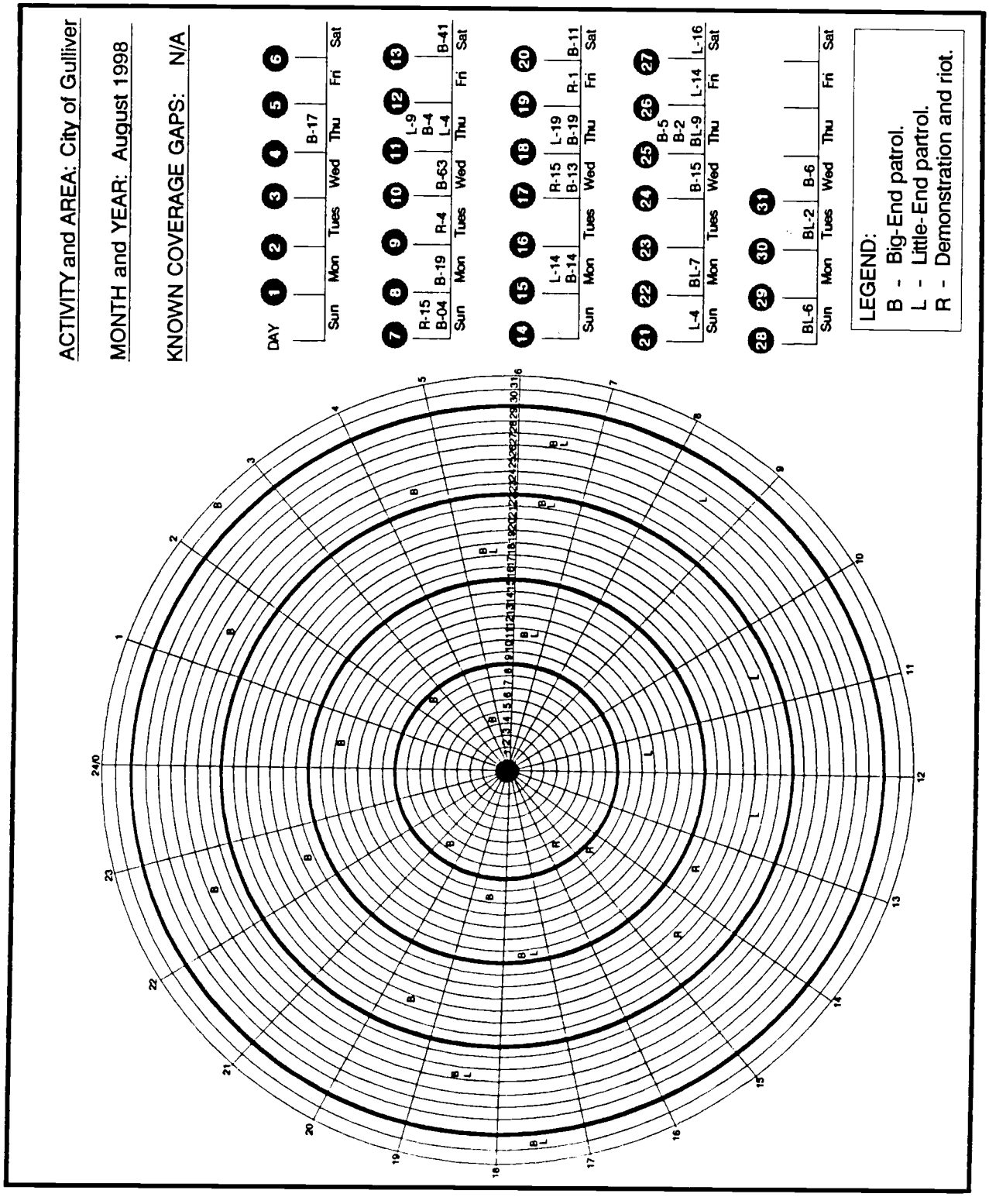

ACTIVITY and AREA: City of Gulliver
MONTH and YEAR: August 1998
KNOWN COVERAGE GAPS: N/A
DAY
Sun Mon Tues Wed Thu Fri Sat
B-17
R-15 B-04 B-19 R-4 B-63 L-9 B-4 L-4 B-41
L-14 B-14 R-15 B-13 L-19 B-19 R-1 B-11
L-4 BL-7 B-15 B-5 B-2 BL-9 L-14 L-16
BL-6 BL-2 B-6
LEGEND:
B - Big-End patrol.
L - Little-End partrol.
R - Demonstration and riot.

Figure 3-4-10. Pattern analysis plot sheet.

Evaluating the information available, we construct a doctrinal template for the operations of both rebel groups, which are similar (Figure 3-4-11). In the margins we include a description of their normal tactics and reactions, as well as HVTs to complete the threat model.

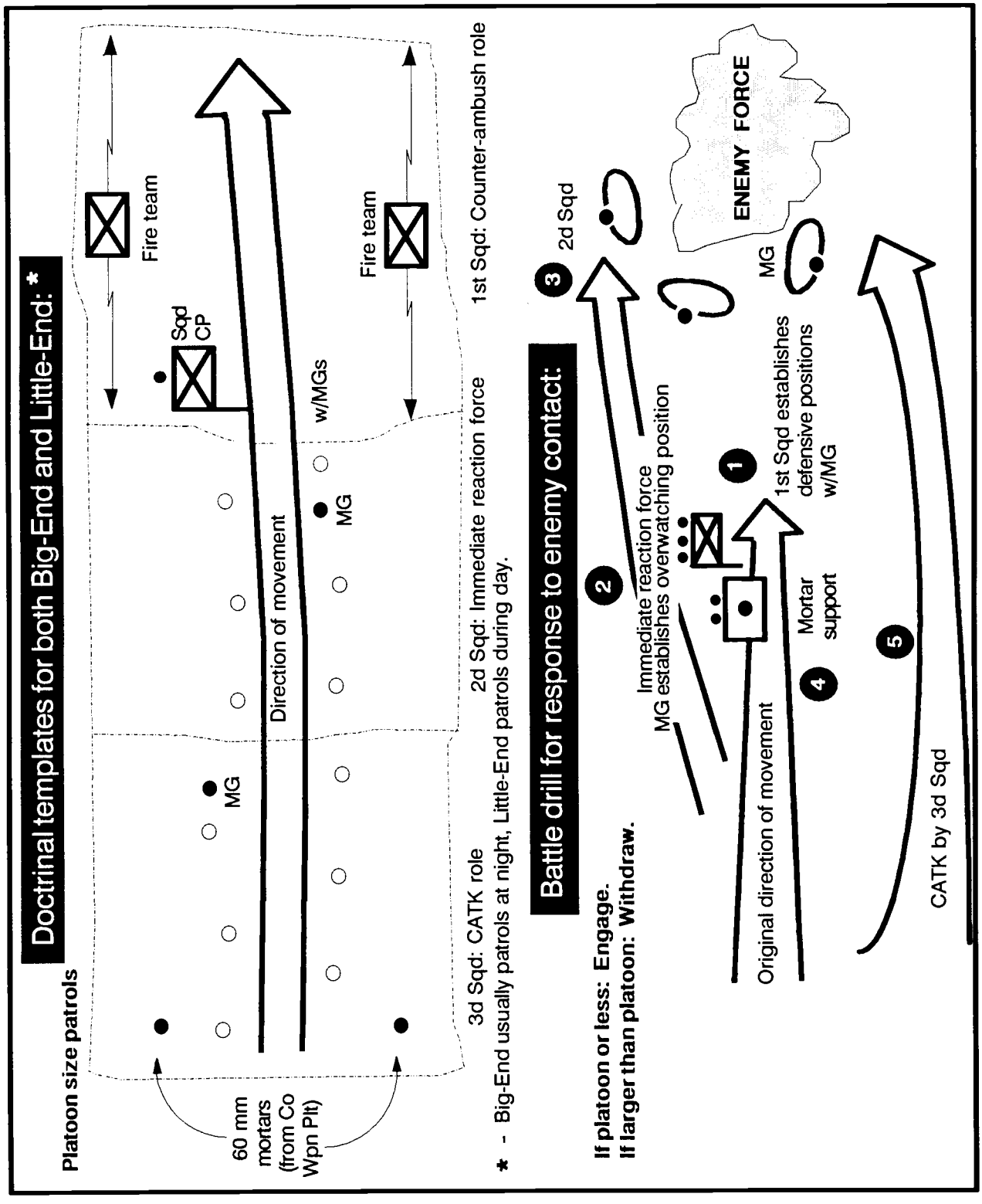


Figure 3-4-11. Threat model of militia operations.

We use similar techniques to template the activities of student demonstrators. Although more difficult, we are able to prepare a graphic depiction of their normal "operations" (Figure 3-4-12).

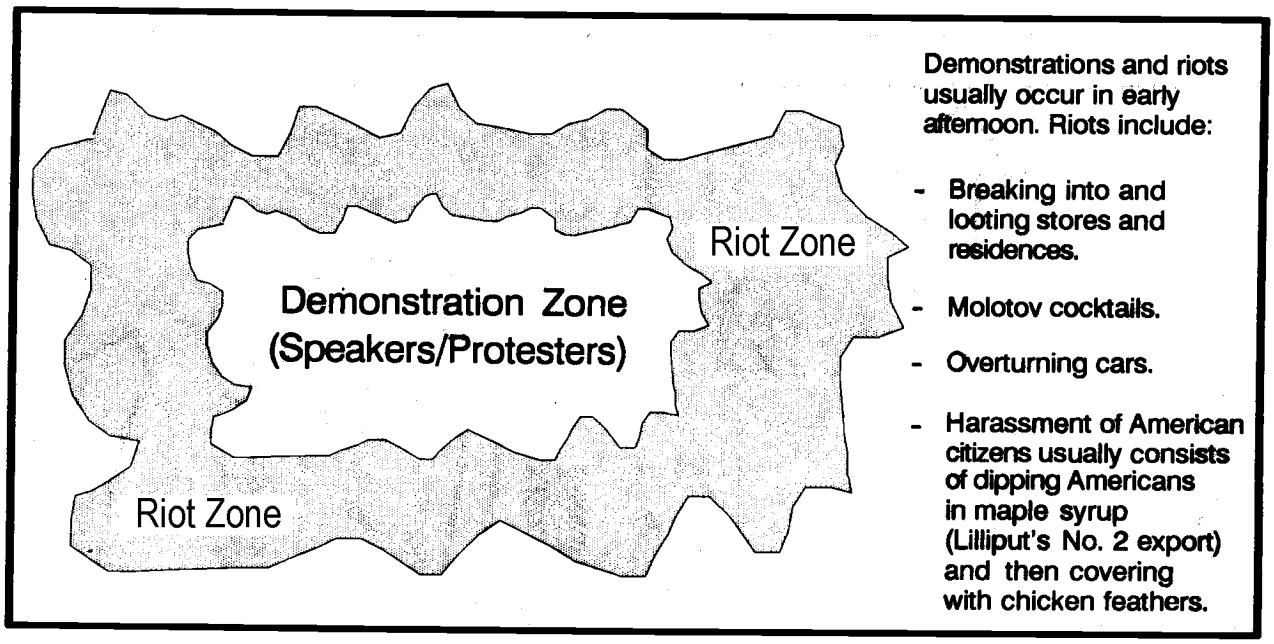

Demonstrations and riots usually occur in early afternoon. Riots include:
- Breaking into and looting stores and residences.
- Molotov cocktails.
- Overturning cars.
- Harassment of American citizens usually consists of dipping Americans in maple syrup (Lilliput's No. 2 export) and then covering with chicken feathers.
Riot Zone
Demonstration Zone (Speakers/Protesters)
Riot Zone

Figure 3-4-12. Threat model of student activities.

DETERMINE THREAT COURSES OF ACTION

We construct a situation template based on the threat models and patterns of recent activity (Figure 3-4-13). It focuses on likely clashes between the two rebel factions and possible demonstrations by the student activists, the most likely threats to accomplishment of our mission. Like a more traditional situation template, the staff uses it during wargaming to evaluate friendly COAs against the potential threats to mission accomplishment.

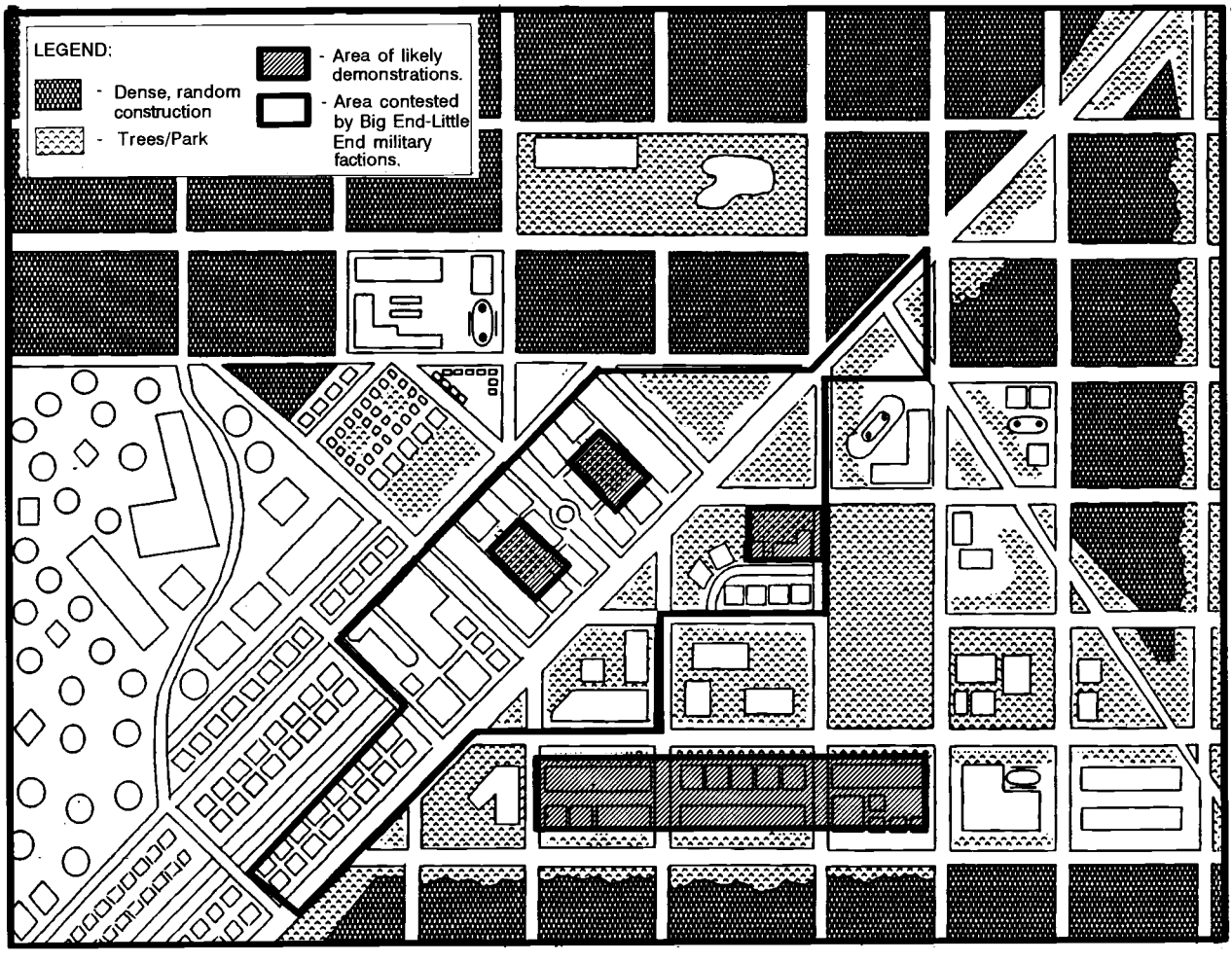

LEGEND:
- Dense, random construction
- Trees/Park
- Area of likely demonstrations.
- Area contested by Big End-Little End military factions.

Figure 3-4-13. Situation template depicting threats to the mission.

The situation template forms the basis for the event template. In this case, the event template depicts NAIs that will alert us of impending clashes between the rival military factions or demonstrations by the students (Figure 3-4-14). The status of the negotiations within the governmental center are included on the event template and in our collection planning, since progress or failure there has a direct bearing on the activity of the two rebel factions.

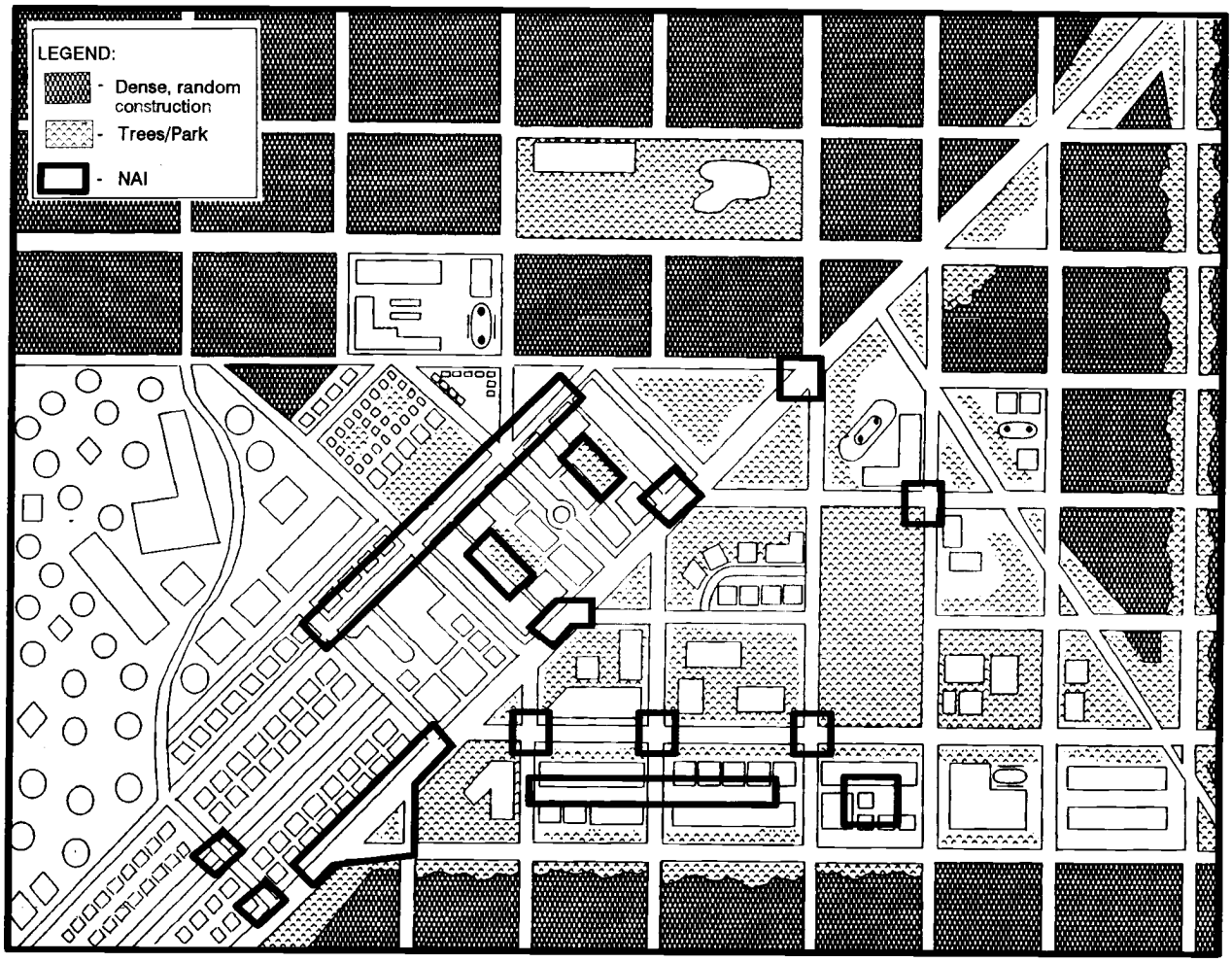


Figure 3-4-14. Event template.

DISSEMINATE, USE, AND REFINE IPB PRODUCTS

As the staff completes the command estimate process and begins planning and executing the friendly COA, we evaluate incoming intelligence against the event and situation templates to quickly identify developing threats. As incoming intelligence confirms or denies the accuracy of our initial assessments and evaluations, we continue to refine and update our IPB.